



天锐绿盾数据防泄密系统(专业版) 管理员使用手册

厦门天锐科技股份有限公司

Xiamen Tipray Technology Co., Ltd

版权声明

本文件以及所提及的数据、图标、名称、所有权皆属于厦门天锐科技股份有限公司所有。未得到厦门天锐科技股份有限公司的书面认可，任何个人或组织均不得以任何手段与形式对本方案内容进行复制、转印和传播。

本文件中的内容，厦门天锐科技股份有限公司拥有最终解释权。

目 录

目 录.....	3
1 概述.....	5
2 系统使用.....	5
2.1 规则中心.....	5
2.1.1 添加、修改、删除操作员类型.....	5
2.1.2 操作员类型配置.....	8
2.1.2.1 受控程序设置.....	8
2.1.2.2 安全选项.....	9
2.1.2.3 特殊文件后缀.....	12
2.1.2.4 外发文件.....	12
2.1.3 自定义程序添加.....	15
2.1.4 添加、修改、删除终端操作员.....	19
2.1.5 操作员权限设置.....	23
2.1.6 登录情况.....	23
2.1.7 密级管理.....	24
2.1.8 智能加密.....	26
2.2 企业密钥.....	31
2.2.1 设置/修改企业密钥.....	32
2.2.2 导入/导出企业密钥.....	32
2.3 密级设置.....	33
2.4 离线策略.....	34
2.5 离线终端.....	37
2.6 全盘加解密.....	39
2.7 全盘加解密记录.....	40
2.8 特殊目录设置.....	41
2.9 批量加解密记录.....	42
2.10 解密文件统计.....	43
2.11 密级转换日志.....	44
2.12 文件备份记录.....	44
2.12.1 查看文件备份记录.....	44
2.12.2 查看备份文件内容.....	45
2.12.3 过滤不需要的文件类型备份.....	46
2.13 外发设置中心.....	48
2.13.1 机器码白名单.....	48
2.13.2 信任软件列表.....	49
2.13.3 外发水印设置.....	51
2.14 文件外发记录.....	54
2.14.1 查看文件外发记录.....	54
2.14.2 查看外发文件内容.....	54
2.15 邮件白名单设置.....	55
2.15.1 收件人白名单.....	55
2.15.2 发件人白名单.....	61
2.16 服务器白名单设置.....	62

2.17 审批流程管理.....	64
2.17.1 审批流程设置.....	64
2.17.2 审批流程分配.....	75
2.17.3 审批日志.....	77
2.18 屏幕水印设置.....	79
2.19 应用安全接入设置.....	83
2.20 U 盘终端管理.....	84
2.21 外发 U 盘.....	87
2.22 穿透加解密.....	90
2.23 主辅 IP 切换.....	91
2.23 独立审批.....	92
2.25 长期未上线终端管理.....	96
2.26 未授权终端.....	99
2.27office 文档水印.....	103

1 概述

天锐绿盾数据防泄密系统（简称：数据防泄密系统）采用文件过滤驱动实现透明加解密，对用户完全透明，不影响用户操作习惯，从源头上保障企业数据安全。通过对电子文档的实时动态保护、操作全程跟踪，对各种可能造成泄密的途径进行控制，防止企业计算机信息被破坏、丢失、泄密。

数据防泄密系统由服务端、控制台和终端三部分组成。服务端安装在长时间开机的服务器电脑上，控制台安装在管理员使用的电脑上，终端程序安装在每个需要文档保护或者需要阅读加密文档的员工电脑上。

2 系统使用

2.1 规则中心

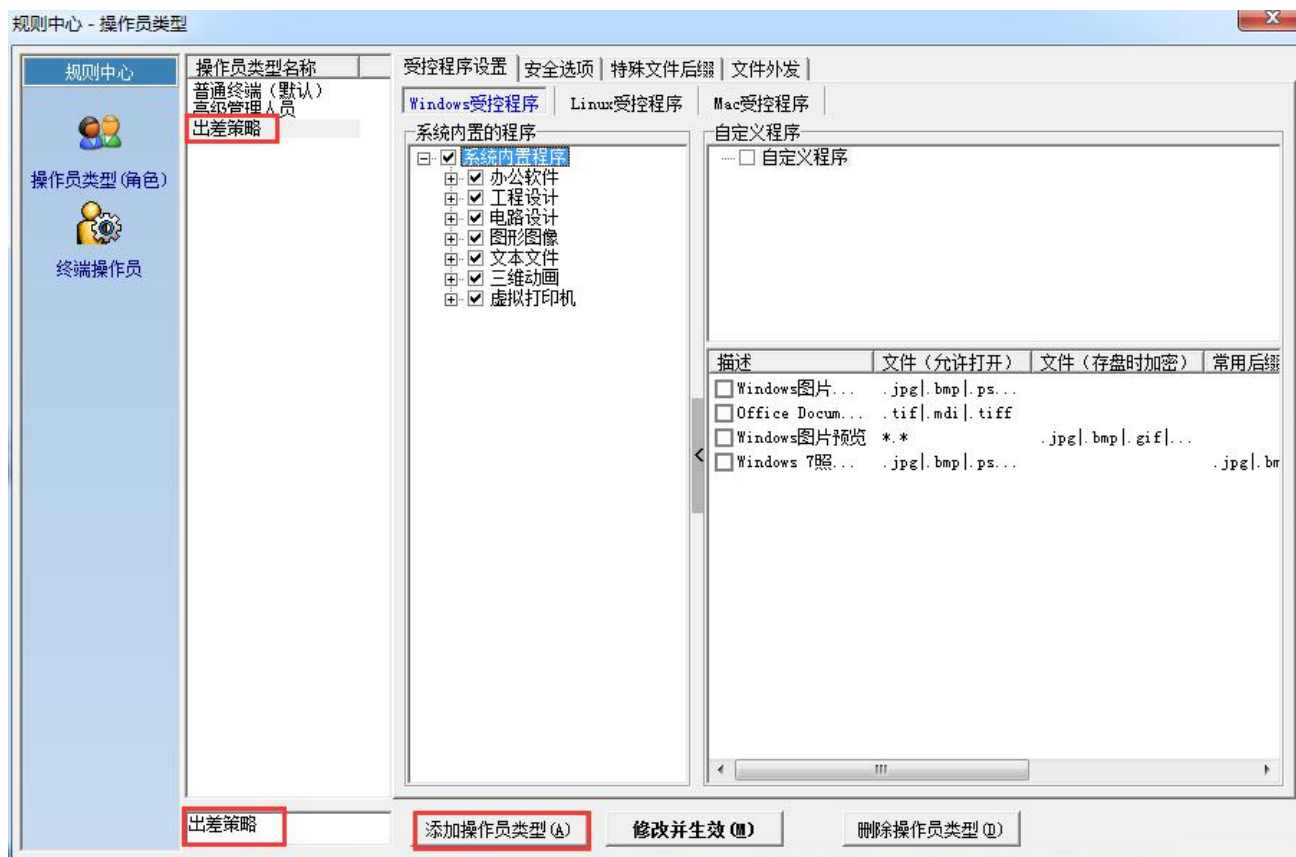
系统加密策略在“规则中心”中进行设置，规则中心包括操作员类型和终端操作员设置。在“操作员类型”中设置 A 操作员类型的加密策略、权限，配置好之后，在“终端操作员”中给 B 操作员分配 A 操作员类型，这样用 B 操作员登录的终端就具有 A 操作员类型的加密策略和权限。

2.1.1 添加、修改、删除操作员类型

操作员类型可以按用户需求进行添加、修改、删除。

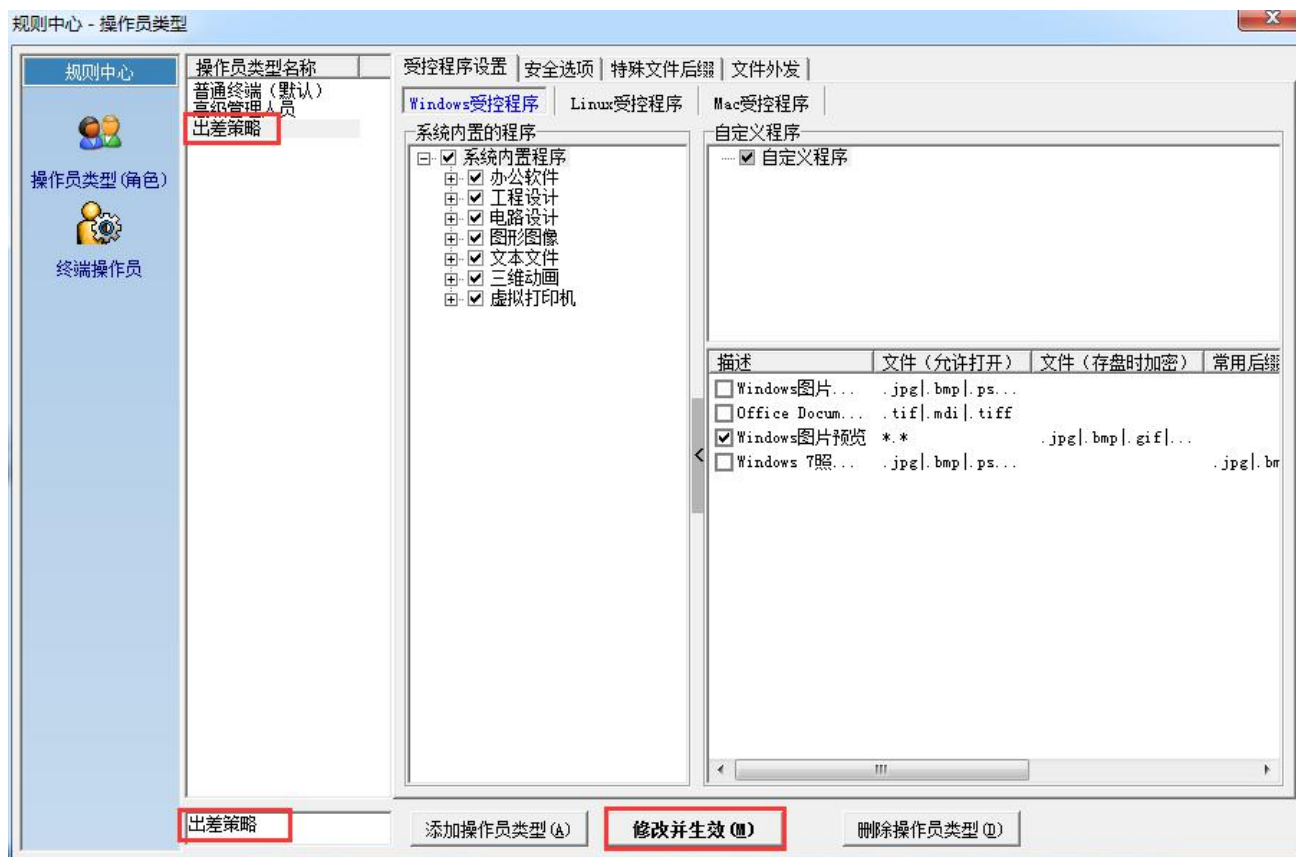
添加操作员类型

在功能栏中选择“文件加密”-“规则中心”，将弹出“规则中心-操作员类型”窗口，在窗口左下方的文本框中输入需要添加的操作员类型名称，然后点击“添加操作员类型”按钮添加。添加完操作员类型后还需根据实际情况，重新配置“受控程序设置”、“安全选项”、“特殊文件后缀”（配置详见“操作员类型配置”），点击“修改并生效”保存。如下图所示：



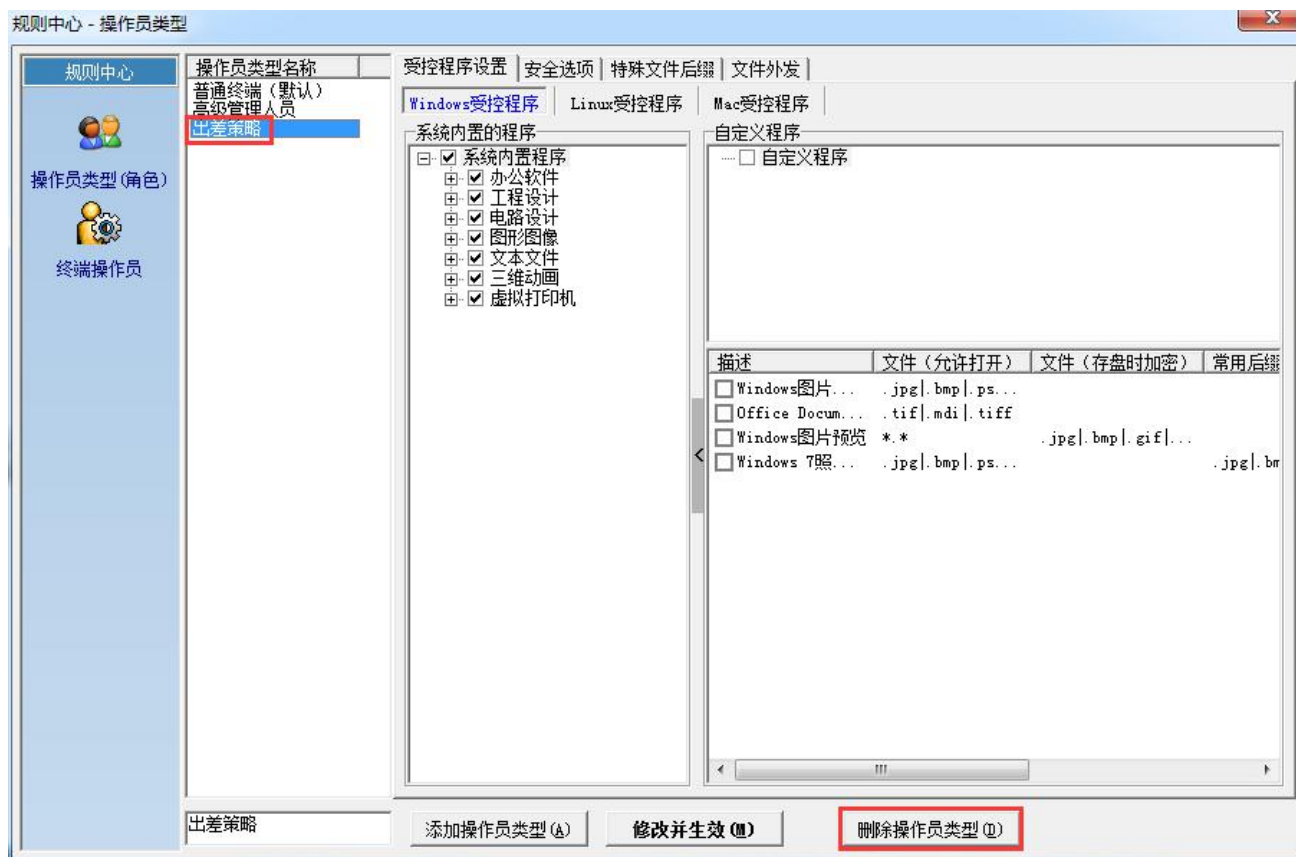
修改操作员类型

在“规则中心-操作员类型”窗口，选中需要修改的操作员类型。如果要修改操作员类型名称，则在窗口左下方的文本框中输入要修改为的操作员类型名称，再点击“修改并生效”按钮。如果要修改配置，则修改“受控程序设置”、“安全选项”、“特殊文件后缀”的相关设置。从一个页面切换到另一个页面前，如果有做修改，需要先保存，即点击“修改并生效”按钮。如下图所示：



删除操作员类型

在“规则中心-操作员类型”窗口，选中需要删除的操作员类型，再点击窗口右下角的“删除操作员类型”按钮即可（删除操作员类型之前请确认是否还有终端操作员属于该操作员类型，如有请先删除或修改属于该操作员类型的操作员）。如下图所示：



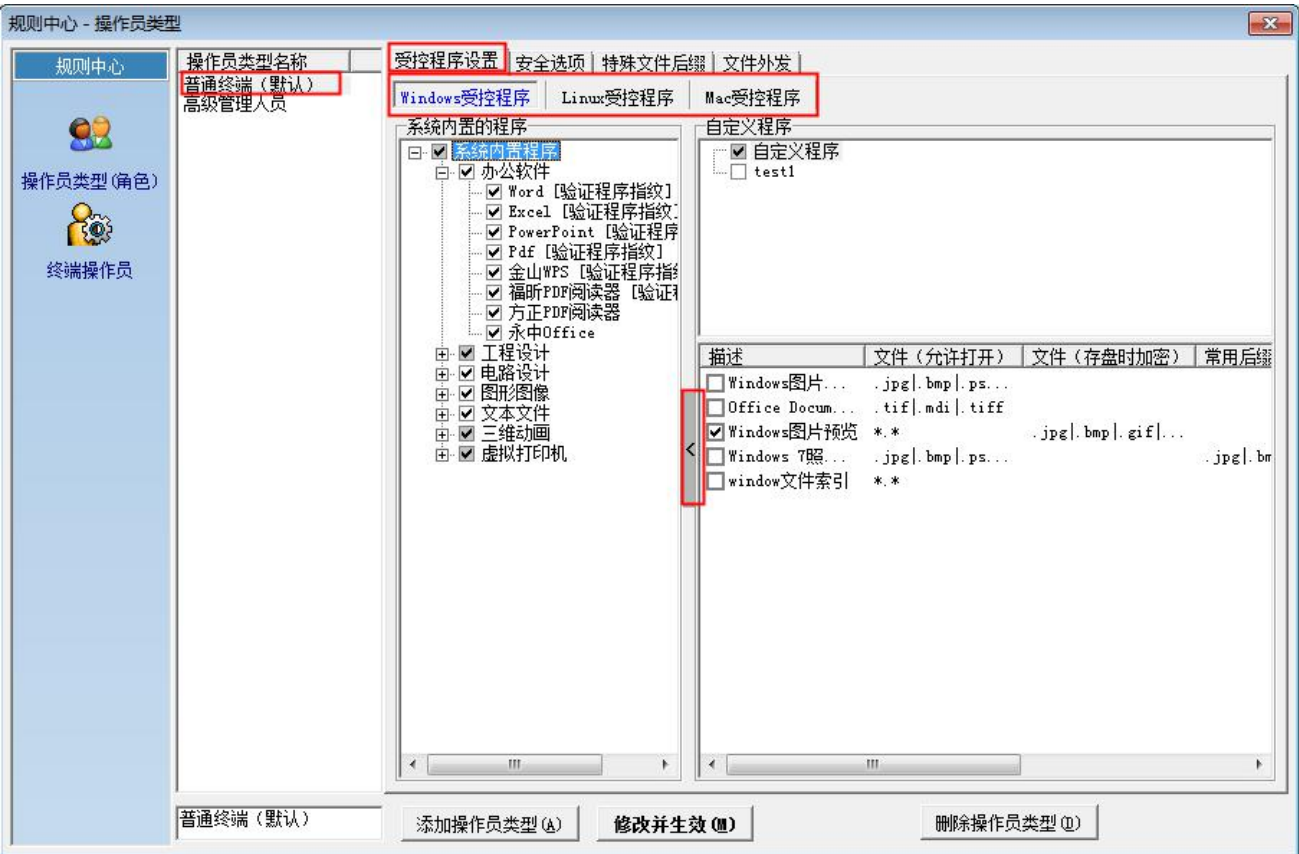
2.1.2 操作员类型配置

配置加密角色的具体策略。系统默认带有的“普通终端”和“高级管理人员”两个角色在加密权限有所不同，可分别适用于普通人员和管理人员。策略可以进行进一步的修改管理。

2.1.2.1 受控程序设置

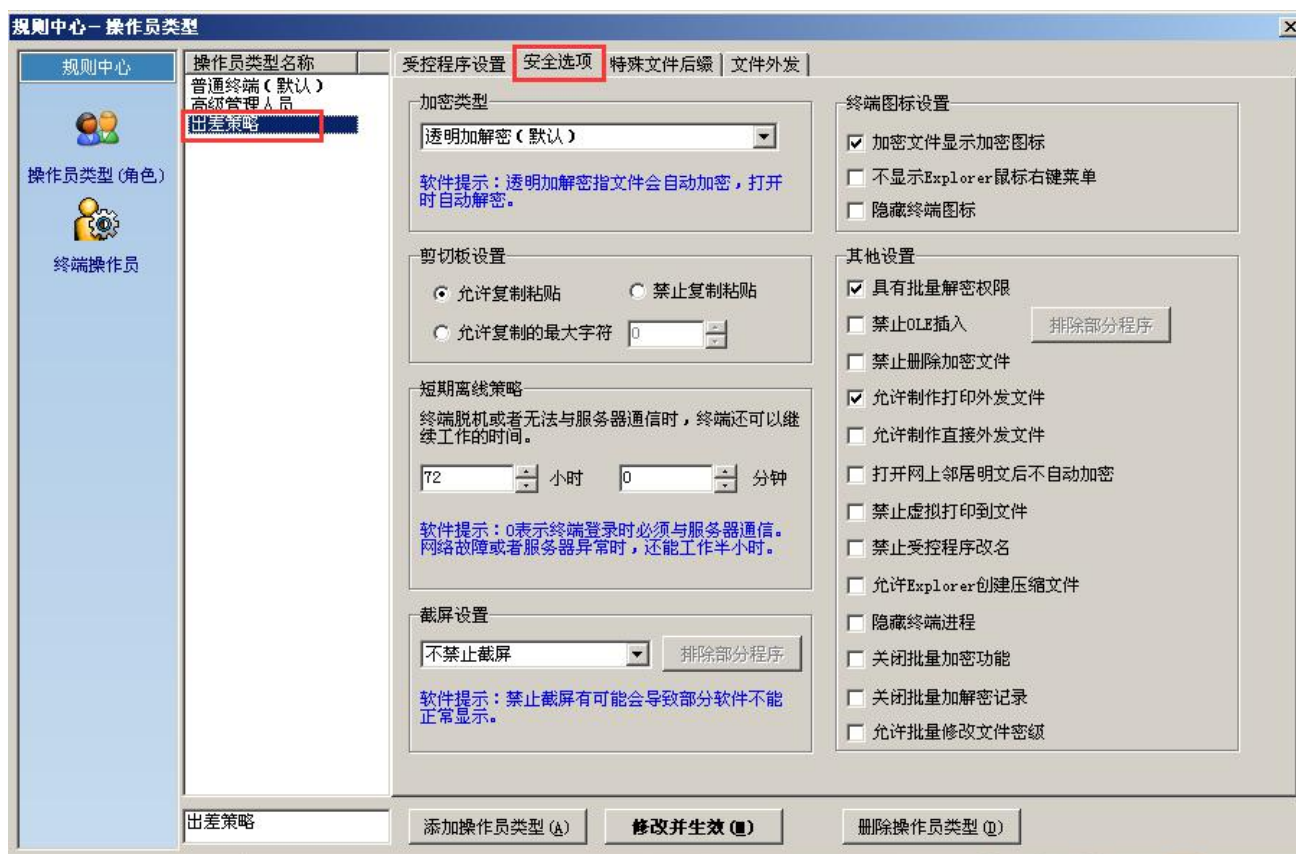
受控程序按照 Windows, Mac, Linux 不同系统分开配置。

设置需要受保护（需要加密）的文件类型：在需要加密的程序前的方框中打钩。系统内置了部分常用应用程序（可以点击收缩按钮进行隐藏），也可以自定义添加受控程序，“自定义程序”支持大部分的文件类型。自定义程序添加方法详见“自定义程序添加”。



2.1.2.2 安全选项

设置操作员类型的加解密模式以及操作权限。



“加密类型”：指该操作员类型的文件加密基本策略，包括“透明加解密（默认）”和“只解密不加密”。“透明加解密”指文件自动加密，打开时自动解密，“只解密不加密”指不加密文件，但可以读加密文件。**注意**：加密类型为“只解密不加密”的终端生成的所有文档都不再加密，对于部分加密文档，重新保存后也可能以明文的形式存储（比如用 Word 阅读加密文档，编辑后保存，将以明文方式保存）。

“剪切板设置”：可以设置对剪切板的数据进行加密或者不加密，还可以限制允许复制的最大字节。设置为剪切板加密，受控程序文件内容之间可以相互复制粘贴，但受控程序文件内容不能复制到非受控程序中，如 Word 为受控，IE 为非受控，Word 文件内容不能复制到 IE 里。

“短期离线策略”：指当终端脱机或者无法与服务器通信时，终端还可以正常加解密文档的时间。默认是 72 个小时，即当终端无法连接服务器时，终端还可以正常工作 72 个小时。

说明：短期离线策略适用于公司内部笔记本电脑的日常移动使用，如每天下班后笔记本电脑带回家，可以在脱离公司网络后的一段时间内正常使用电脑上的加密文件。还可以用于处理一些特殊情况，如服务器关机或发生故障导致终端不能与服务器通信时，终端还可以在一段时间内正常进行文件的加解密（解密是针对有批量解密权限的终端，没有权限的无法申请解密），确保办公不会因此中断。短期离线策略是和操作员类型绑定的，不用每次都设置（比如笔记本电脑每天可以直接带回家，而不用申请离线，离线时间从与服务器断开通信时计起）。

“截屏设置”：可以设置为“不禁止截屏”、“禁止使用 PrtScr 键”、“禁止截屏”、“打开加密文件时禁止截屏”。其中禁止截屏和打开加密文件时禁止截屏可以设置部分软件允许使用，选择其后“排除部分程序”进行设置即可。

注意：1.禁止截屏有可能会部分软件不能正常显示。

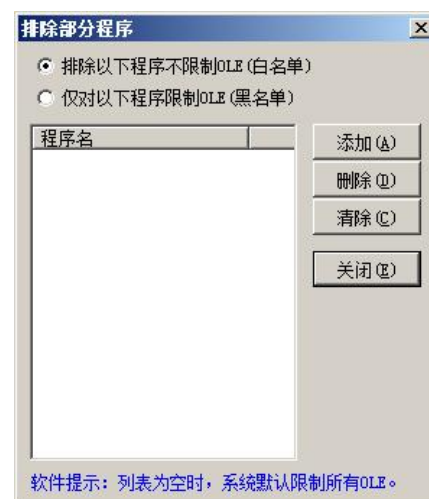
2.将窗口拖拽到桌面边缘或其他窗口遮挡不属于隐藏窗口

“终端图标设置”：可以选择是否显示文件加密图标、任务栏终端图标、explorer 鼠标右键菜单。

“具有批量解密权限”：选择后该操作员类型的终端操作员具有批量解密的权限；

“禁止 OLE 插入”：选择后该操作员类型的终端操作员将不能在应用程序（如 Word、Excel 等）里通过插入对象的方法将加密文档另存为明文文档，或点击 Word 等菜单栏中的“文件”

- “发送”将文件通过 outlook 发到企业外部。可以排除部分程序，使之不受此限制。可设置程序排除白名单和黑名单，如右图所示：



“禁止删除加密文件”：选择后该操作员类型的终端操作员不能删除加密文件；

“允许制作打印外发文件”：选择后该操作员类型的终端操作员可以制作打印外发文件(可以控制打印外发文件的打开次数、使用时间、打开时是否需要密码、是否只能在一台电脑上打开等)，若没有该权限，终端用户需要申请打印外发；

“允许制作直接外发文件”：选择后该操作员类型的终端操作员可以制作直接外发文件(可以控制直接外发文件的打开次数、使用时间、打开时是否需要密码、是否只能在一台电脑上打开等)；

“打开网上邻居明文后不自动加密”：选择后该操作员类型的终端操作员打开共享目录下的文件不会加密；

“禁止虚拟打印到文件”：选择后该操作员类型的终端操作员虚拟打印的文件自动加密，防止虚拟打印成明文；

“禁止受控程序改名”：选择后不允许终端受控程序改名，或其他进程改名为受控程序，区分是否假冒，比如把 Word 设置为受控程序，如果把 Word 的可执行文件 WINWORD.EXE 改名为其他名称，在没有启用“禁止受控程序改名”功能时，软件不会被结束掉，启用后假冒的进程会被结束掉；

“允许 Explorer 创建压缩文件”：选择后可以通过右键菜单创建压缩文件；

“隐藏终端进程”：选择后终端电脑的任务管理器里将不显示天锐绿盾终端进程，起到进程保护的作用；

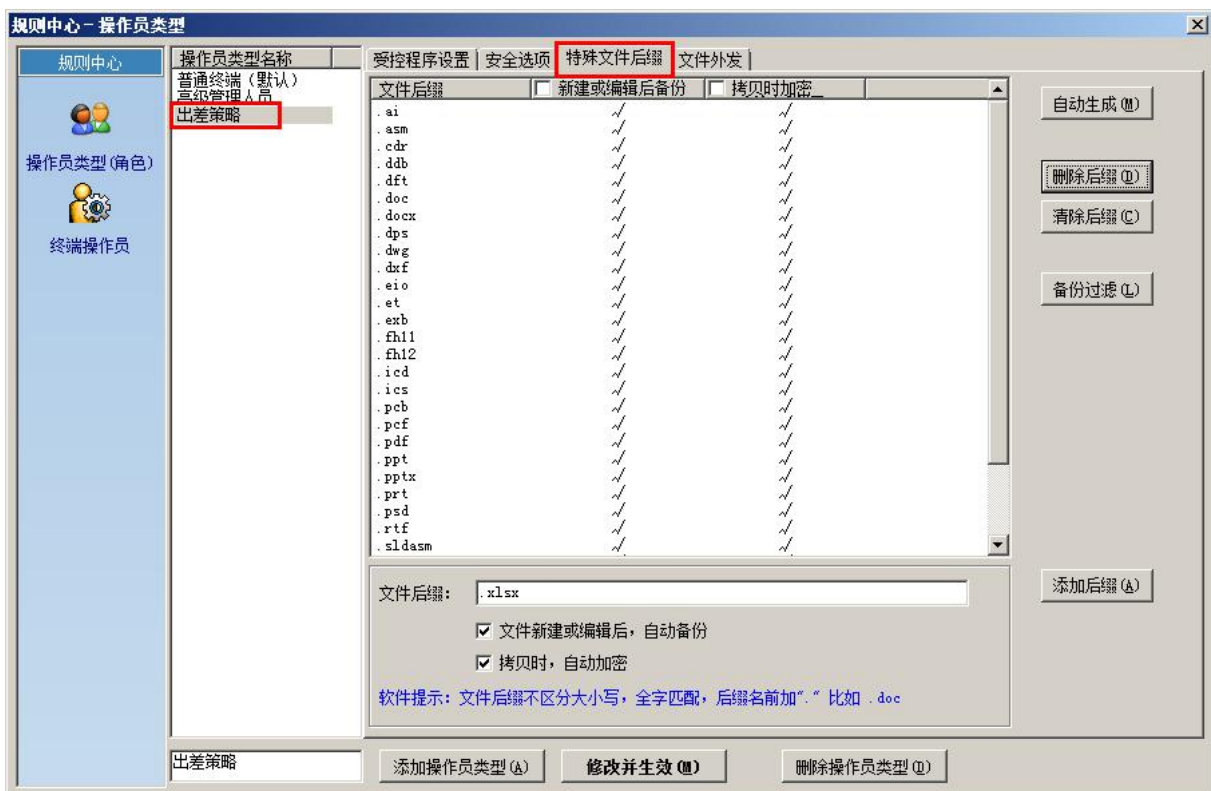
“关闭批量加密功能”：选择后该操作员类型的终端操作员不能进行批量加密文件；

“关闭批量加解密记录”：选择后不记录终端的文件加解密记录。

“允许批量修改文件密级”：选择后该操作员类型的终端操作员可以对文件进行密级转换。

2.1.2.3 特殊文件后缀

在“特殊文件后缀”窗口中，可以设置创建或编辑时需要自动备份、拷贝时需要自动加密的文件后缀。选中某一操作员类型，点击窗口右侧的“自动生成”按钮，系统会根据已设置的受控程序自动生成文件后缀。如果不想设置文件自动备份和拷贝加密，点击“清除文后缀”按钮，然后单击“修改并生效”保存设置。如下图所示：

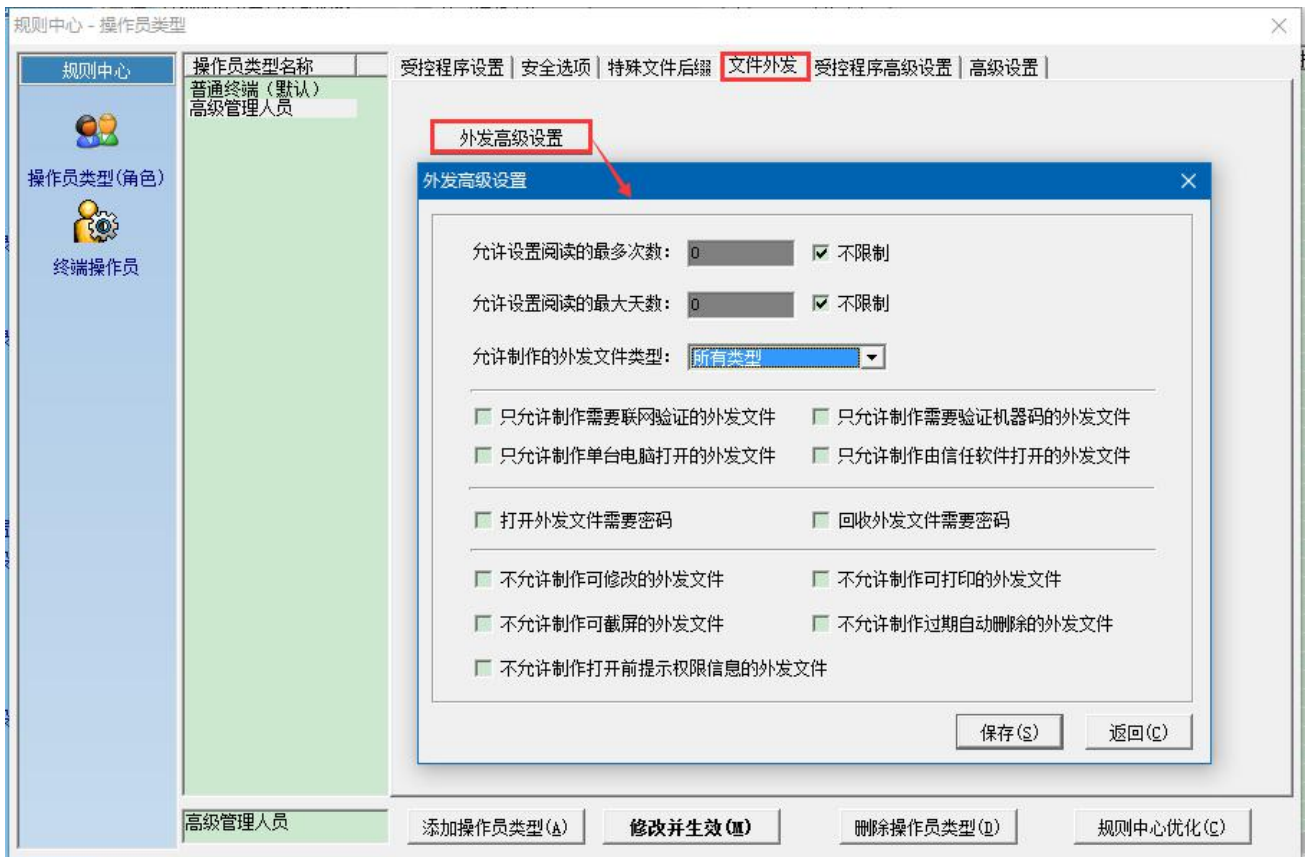


2.1.2.4 外发文件

外发参数设置

在“文件外发”页面选项中，可以对外发文件的权限参数进行设置，设置好外发文件参数

后，终端制作外发文件时，默认的参数将遵循这边的设置。



“允许设置阅读的最多次数”：制作的外发文件允许阅读的次数不能超出该设定值；

“允许设置阅读的最大天数”：制作的外发文件允许打开的时间天数不能超出该设定值；

“允许制作的外发文件类型”：直接外发文件包含两种类型：.ldm 和.exe，可以限制只允许制作其中的一种类型，默认为所有类型；

“只允许制作需要联网验证的外发文件”：制作的外发文件需要联网验证；

“只允许制作单台电脑打开的外发文件”：制作的外发文件只能在一台电脑上打开；

“只允许制作需要验证机器码的外发文件”：制作的外发文件都需要验证机器码后才能打开；

“只允许制作由信任软件打开的外发文件”：制作的外发文件只能使用信任软件才能打开；

“打开外发文件需要密码”：制作的外发文件需要输入设定的密码才能打开；

“回收外发文件需要密码”：制作的外发文件需要输入设定的密码才能回收成功。

“不允许制作可修改的外发文件”：制作的外发文件都不能修改；

“不允许制作可打印的外发文件”：制作的外发文件都不能打印；

“不允许制作可截屏的外发文件”：制作的外发文件都禁止截屏；

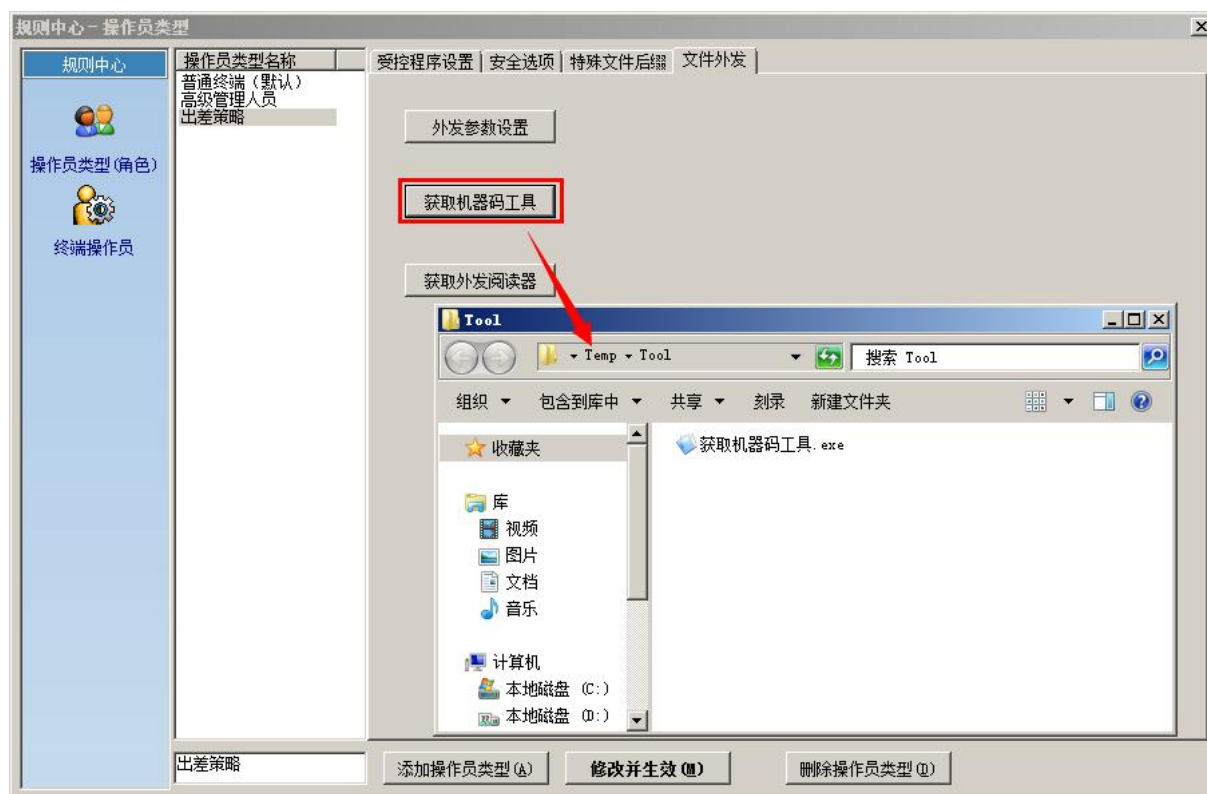
“不允许制作过期自动删除的外发文件”：制作的外发文件不能过期自动删除；

“不允许制作打开前提示权限信息的外发文件”：设置的外发文件打开时不能提示权限信息；

获取机器码工具

如果合作单位是经常往来的诚信单位，可以把合作单位电脑机器码设置为外发机器码白名单（由管理员添加）。在制作直接外发文件的时候，就可以把该机器码添加到外发文件的内置机器码中，这样该电脑打开该直接外发文件的时候就不需要验证机器码就能直接打开，而其他电脑仍需要验证机器码后才能打开。

外发机器码需要使用专门的机器码工具来获取。机器码工具获取方法：在“规则中心-操作员类型”-“文件外发”窗口，鼠标单击“获取机器码工具”按钮，系统自动弹出带有“获取机器码工具.exe”程序的 Tool 文件夹。如下图所示：

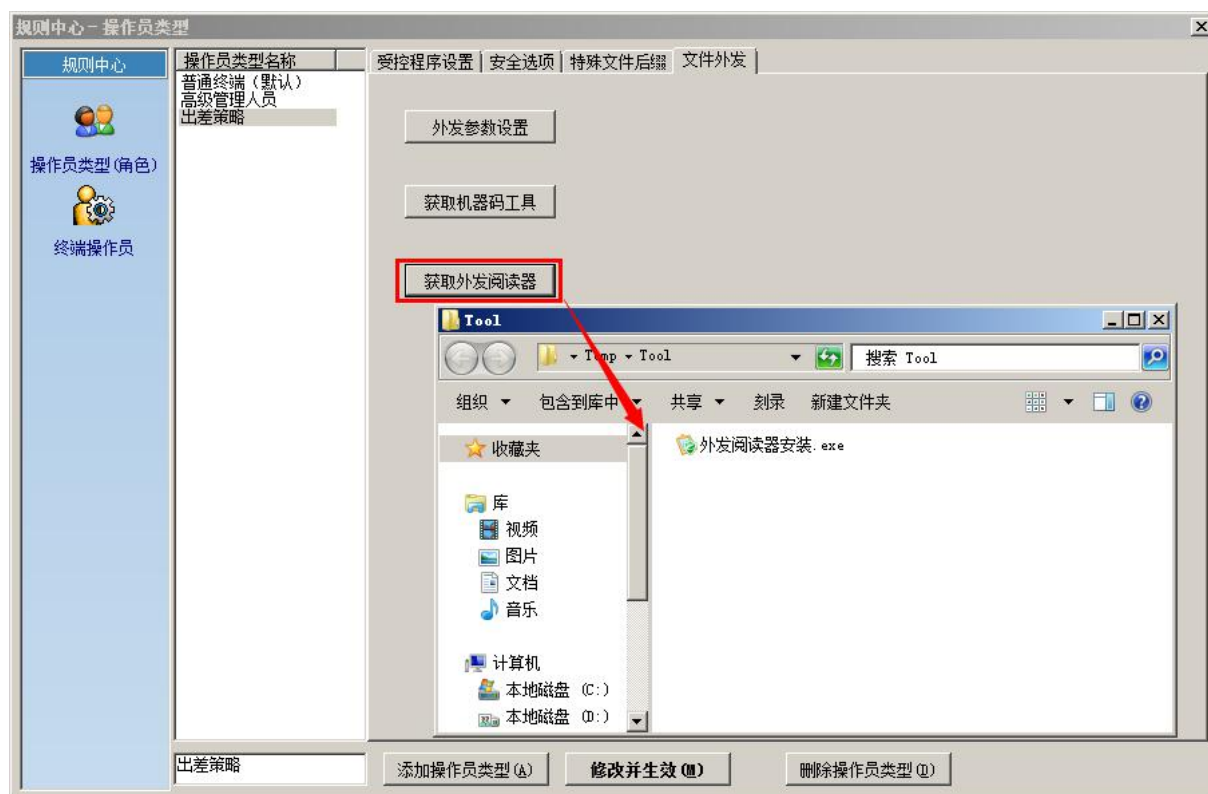


获取外发阅读器

如果制作的直接外发文件后缀为.ldm 格式，打开时需要先安装外发文件阅读器才能打开，因此第一次给合作单位发.ldm 格式的直接外发文件时，需要同时发送“外发阅读器安装.exe”程序。安装外发文件阅读器程序时需要管理员权限才能安装成功，该程序只需安装一次即可，不用每次都安装。

外发阅读器获取方法如下：在“规则中心-操作员类型”-“文件外发”窗口，鼠标单击“获

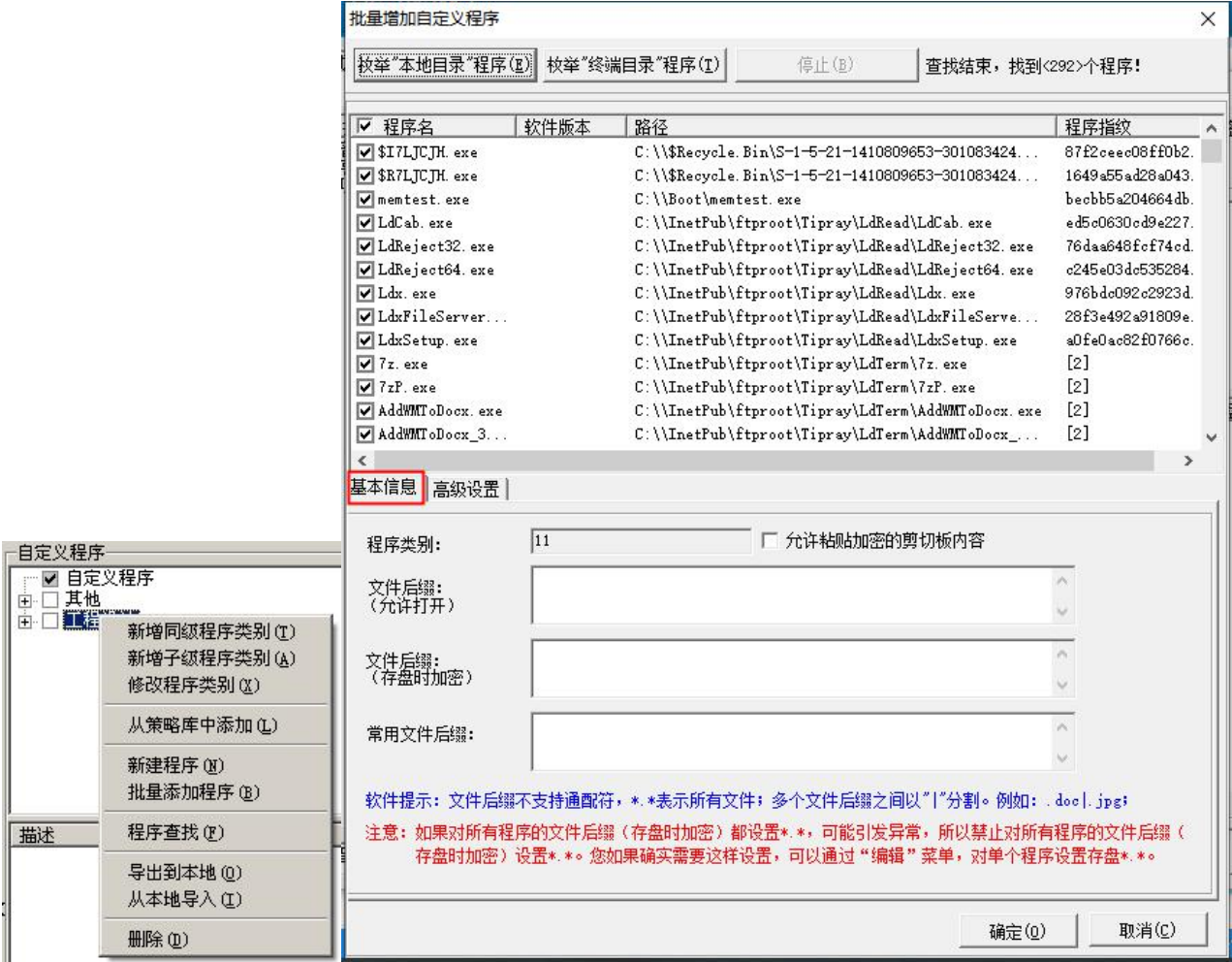
取外发阅读器”按钮，系统自动弹出带有“外发阅读器安装.exe”程序的 Tool 文件夹。如下图所示：

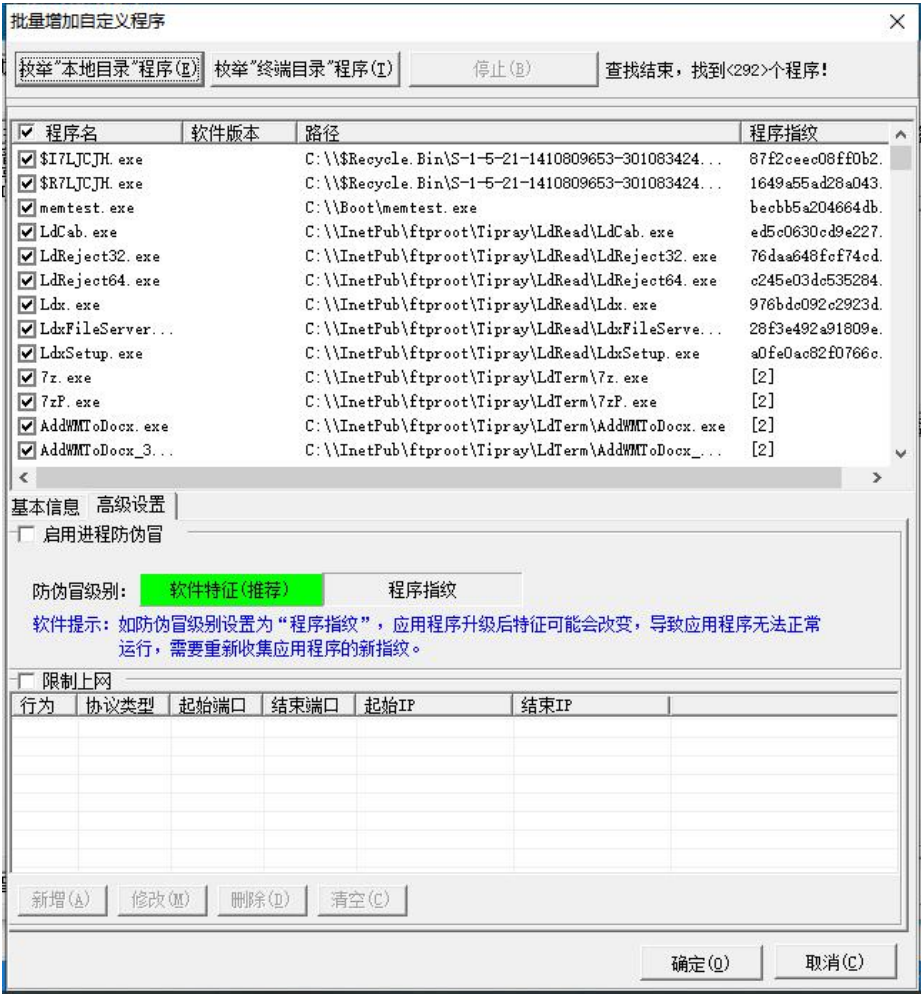


2.1.3 自定义程序添加

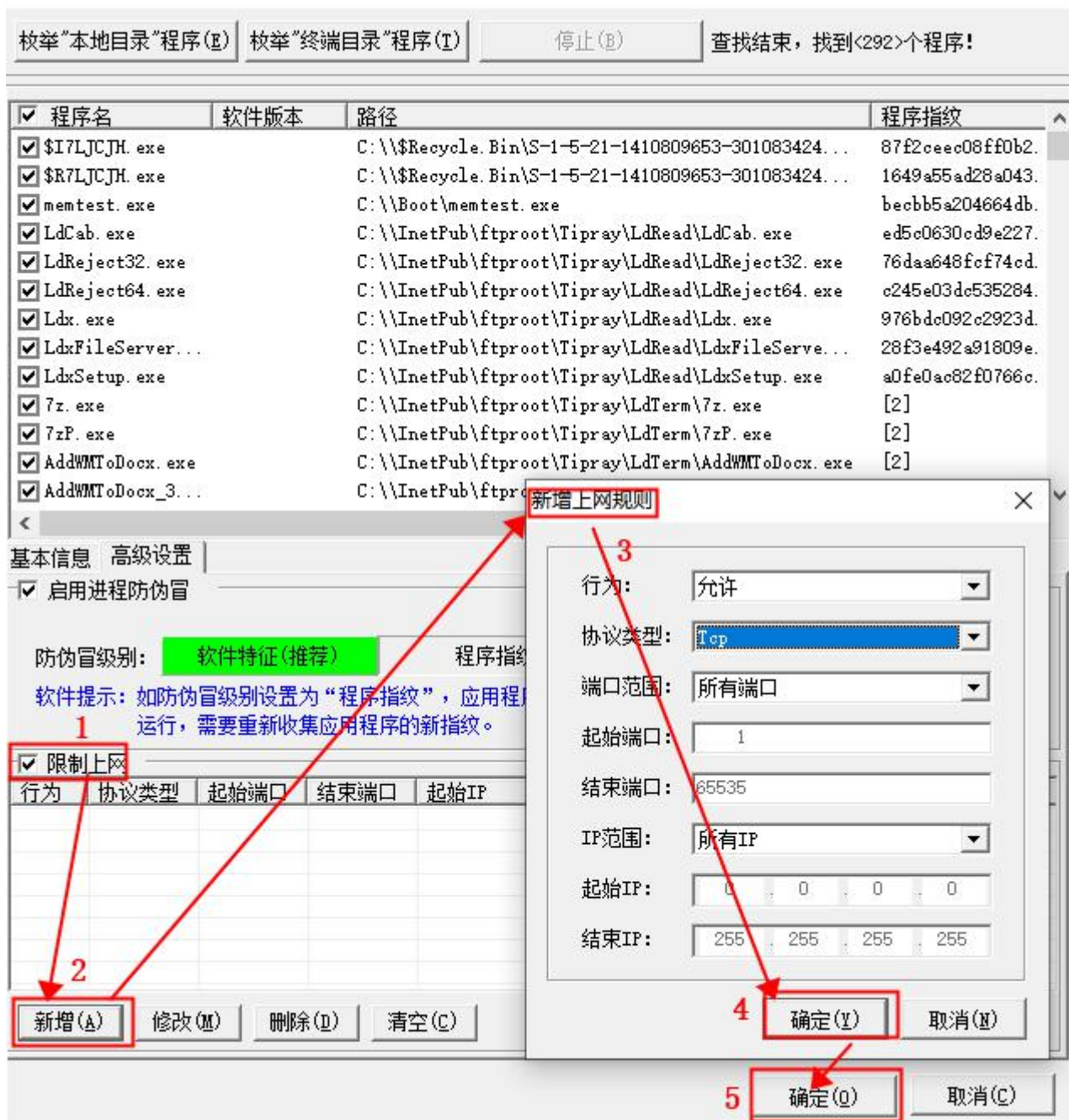
在规则中心-操作员类型-受控程序设置界面的自定义程序中，右键鼠标选择新建同级/子级程序类别，在弹出的窗口中输入程序类别名，类别名最好以软件名称+软件版本号来命名。输入完毕点击“OK”，然后右键该程序类别-批量添加程序，弹出“批量增加自定义程序”窗口，单击“枚举指定目录程序”按钮，选择该软件的安装目录，软件会自动识别程序的可执行程序。一些包含 ..setup.. ..install.. ..uninstall.. 的.exe 程序是软件的安装向导程序，这些不能添加为受控，否则程序安装目录可能会被加密，导致软件安装或运行失败，去掉这些程序。一些明显跟软件正常使用不相关的程序也可以去掉，不能确定的程序先保留，文件后缀（允许打开）设置为*.*，文件后缀（存盘时加密）输入需要加密的文件后缀，多个文件后缀之间以“|”分割，可设置为*.*（加密该程序生成的所有文件），常用文件后缀可暂时不设置。勾选“允许粘贴加密的剪切板内容”，这样在“剪贴板设置”为“禁止复制粘贴”时其他加密文档的内容就可以复制到该程序中；选择“高级设置”勾选“启用进程防伪冒”选择防伪冒级别包括软件特征（默认选项）、程序指纹，启用进程防伪冒即使终端将非受控进程改名为受控进程也无法打开

加密文件。勾选“限制上网”，点击“新增”弹窗“新增上网规则”弹窗，设置选中进程的上网规则，则该进程只有满足设置的规则条件才可上网。如下图所示：





批量增加自定义程序



“允许打开”：可以打开的加密文件后缀；

“存盘时加密”：需要加密的文件后缀；

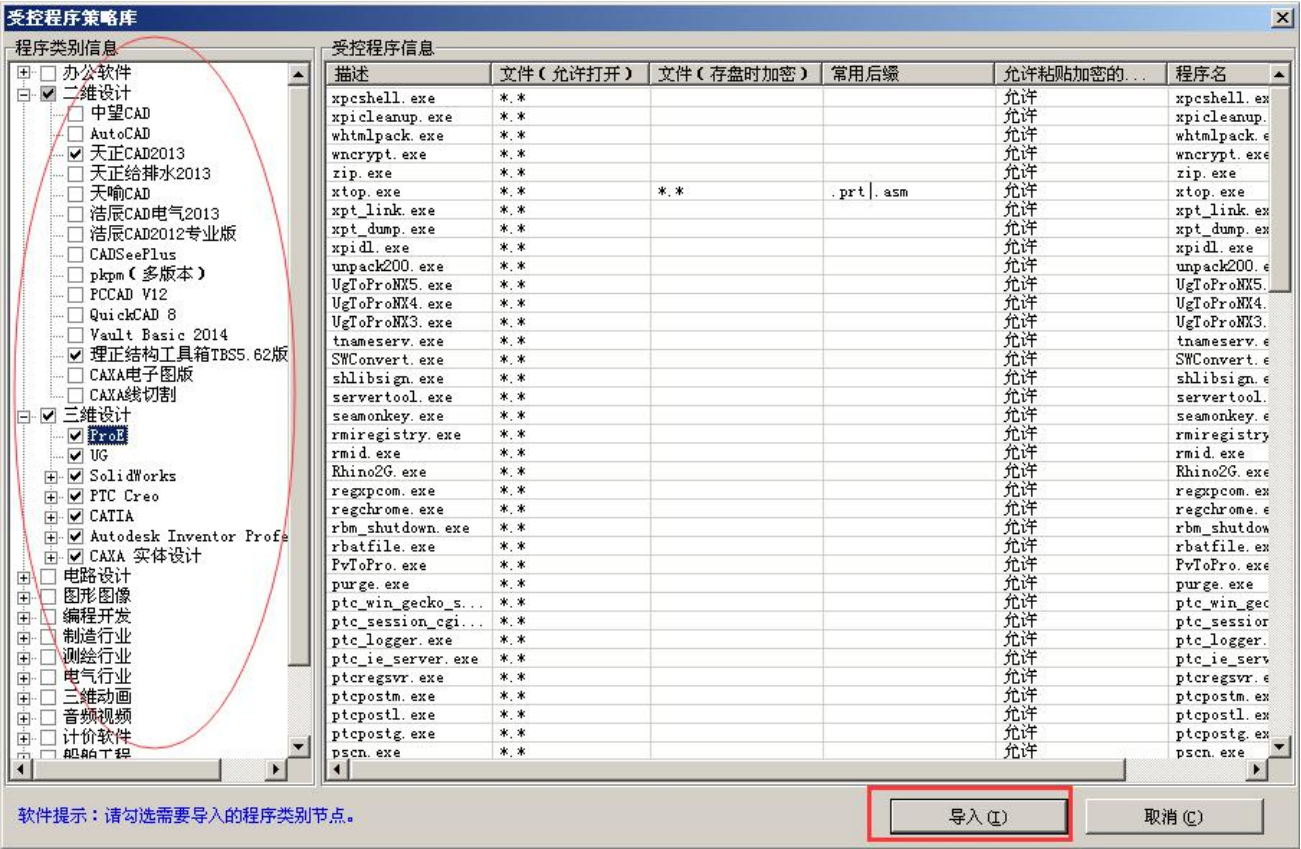
“常见文件后缀”：打开文件不做编辑就会加密。

添加设置完毕点击确定，返回到自定义程序界面，把刚才那些不确定的程序的“存盘时加密”文件后缀置空，不设置（双击该程序或右键程序-编辑来进行修改）。修改完之后，点击“修改并生效”按钮。自定义程序添加好之后还未生效，选中需要添加该程序为受控程序的操作员类型，然后再勾选该自定义程序，“修改并生效”即可。

说明：如果服务器上没有安装该软件，可以把其他电脑上的该软件的安装目录共享或拷贝到服务端，

然后再枚举指定该目录。

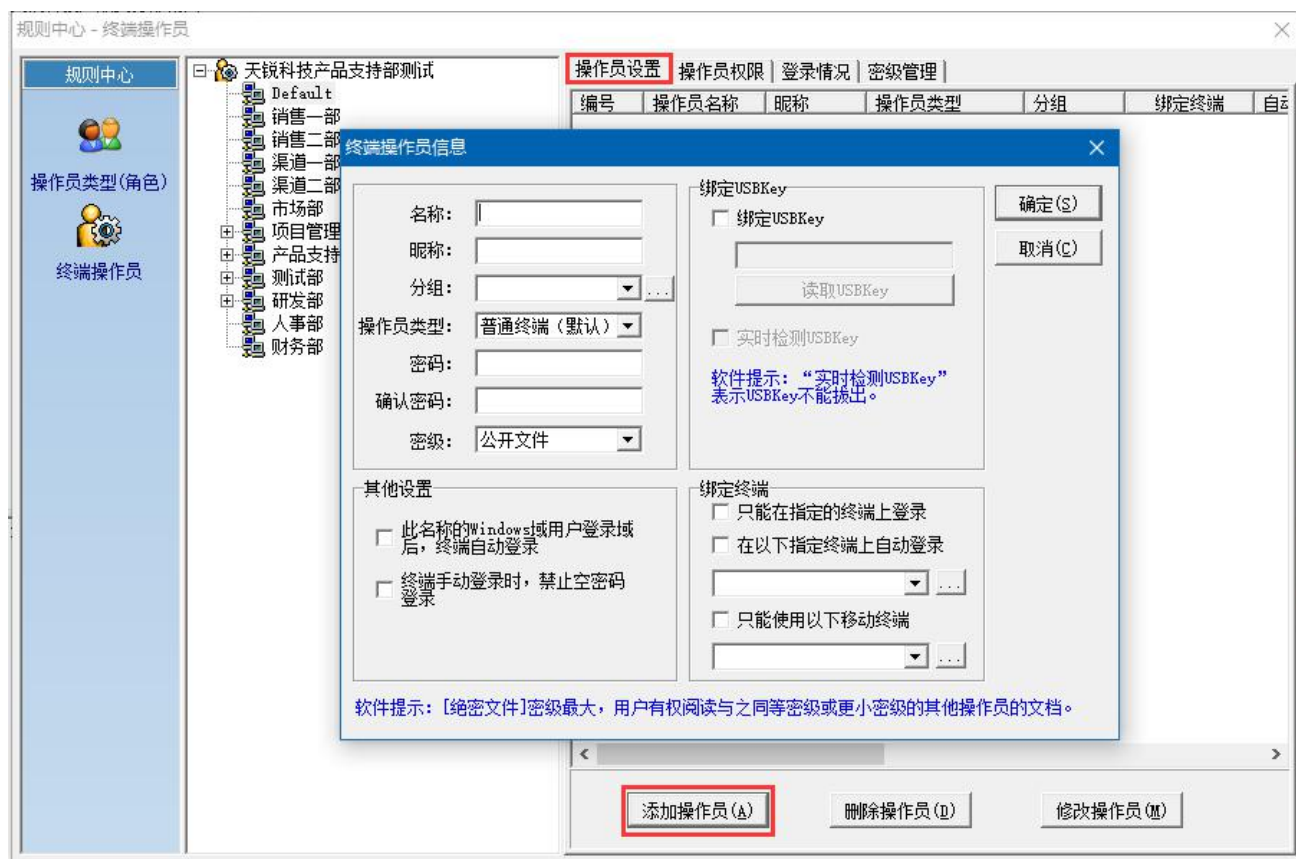
此外，还支持添加策略库功能：在“自定义程序”中，右键鼠标选择“从策略库中添加”，弹出“受控程序策略库”界面，在左侧“程序类型信息”中勾选要增加的受控程序策略，点击导入即可。如下图所示：



2.1.4 添加、修改、删除终端操作员

管理员可以根据需要添加、修改、删除终端操作员。

添加终端操作员：在功能栏选择“文件加密”-“规则中心”，在弹出的“规则中心-操作员类型”窗口中点击“终端操作员”，在“规则中心 - 终端操作员”窗口下方点击“添加操作员”按钮，在弹出的“终端操作员信息”窗口中输入相应的操作员名称、昵称、分组、操作员类型、密码、密级和设置是否绑定 USBKey，是否绑定终端（一个终端只能绑定一个终端操作员），设置完毕点击“确定”。如下图所示：



“绑定 USBKey”：指终端操作员登录时，是否需要插入指定的 USBKey 作为身份识别。其中“实时检测 USBKey”是指，终端操作员登录后，USBKey 不能拔出，否则将不能加解密文档。

“只能在指定的终端上登陆”：指该终端操作员只能在指定的终端电脑上登录。

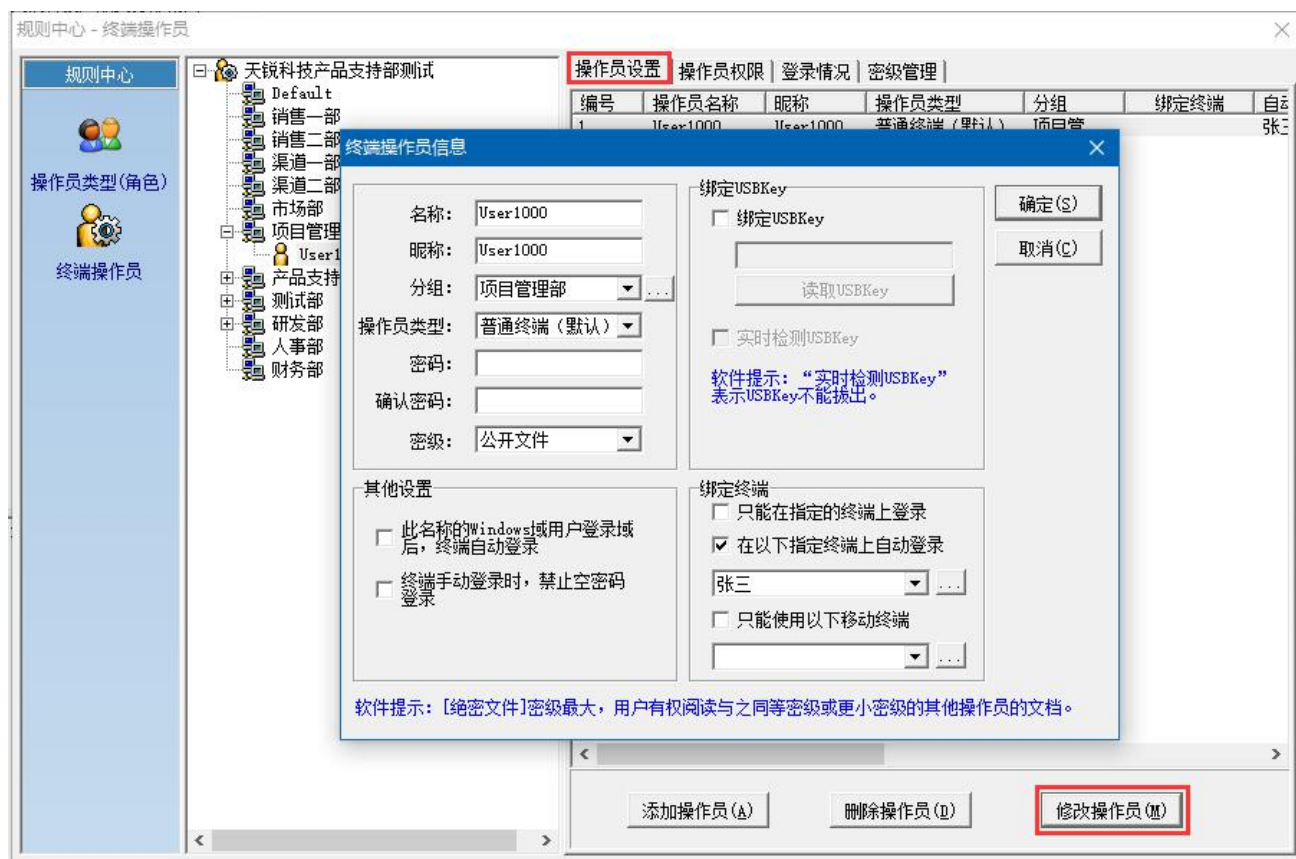
注意：每个终端电脑的识别依赖于终端电脑的硬件标识，终端电脑硬件发生变化时，有可能会重新生成新的终端节点，此时需要重新绑定操作员，否则将导致终端无法登录。

“在指定终端上自动登录”：指定的终端启动时使用该终端操作员自动登录。如果终端不绑定操作员，终端每次需要手动登录，且可以用不同的操作员登录。

“只能使用以下移动端”：指终端操作员只能在指定移动终端上登录。

“其他设置”：可以设置此名称的 Windows 域用户登录域后，该名称的终端自动登录；可以设置终端手工登录时，禁止空密码登录。

修改终端操作员：在“规则中心-终端操作员”窗口，在终端操作员表中选中需要修改的终端操作员，然后点击“修改操作员”按钮，在弹出的“终端操作员信息”对话框中修改操作员名称、昵称、分组、操作员类型、密码、密级和设置是否绑定 USBKey，是否绑定终端。如下图所示：



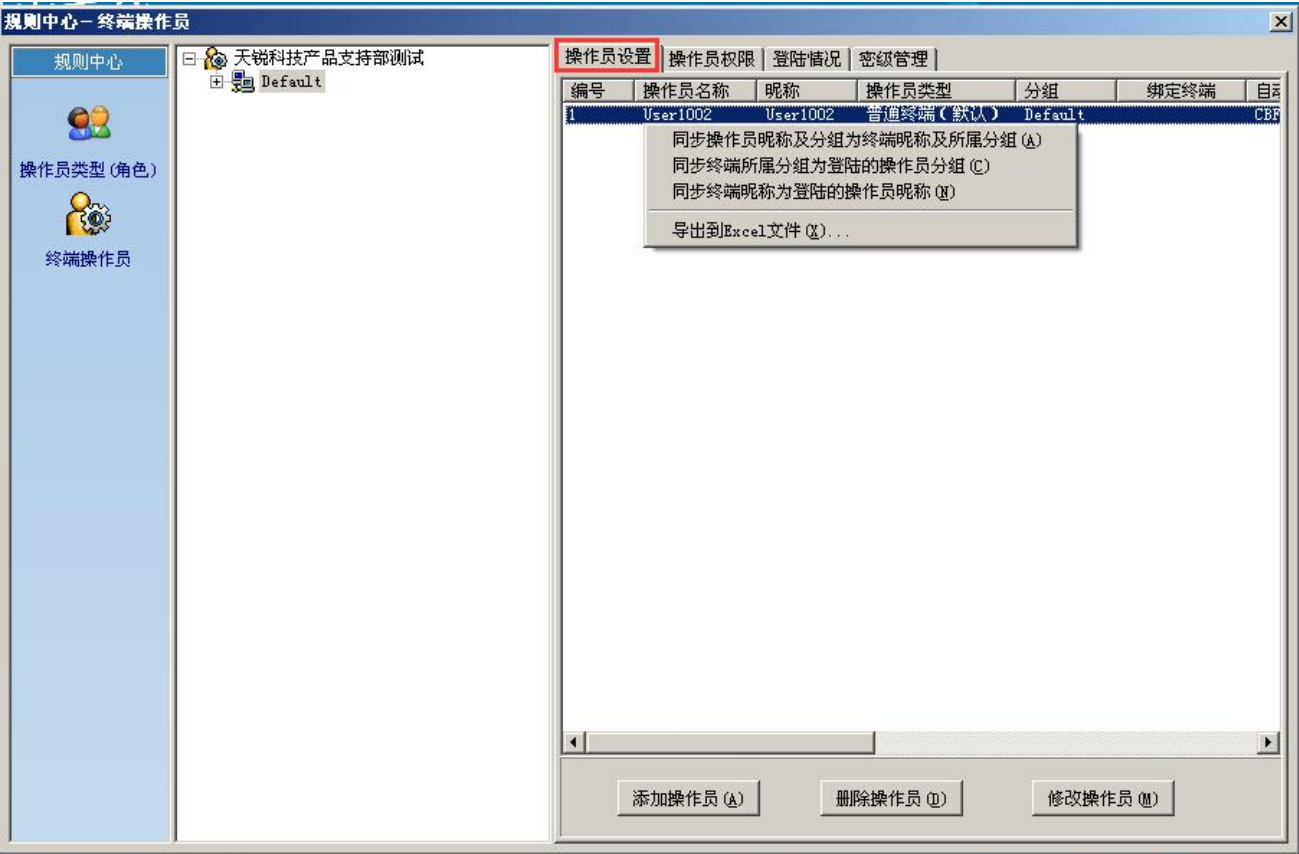
提供三种方式同步操作员或终端的昵称或分组信息：

“根据绑定的终端同步操作员昵称及分组”：对于绑定了终端的操作员，可以同步其昵称及分组为绑定的终端的昵称及所属分组。

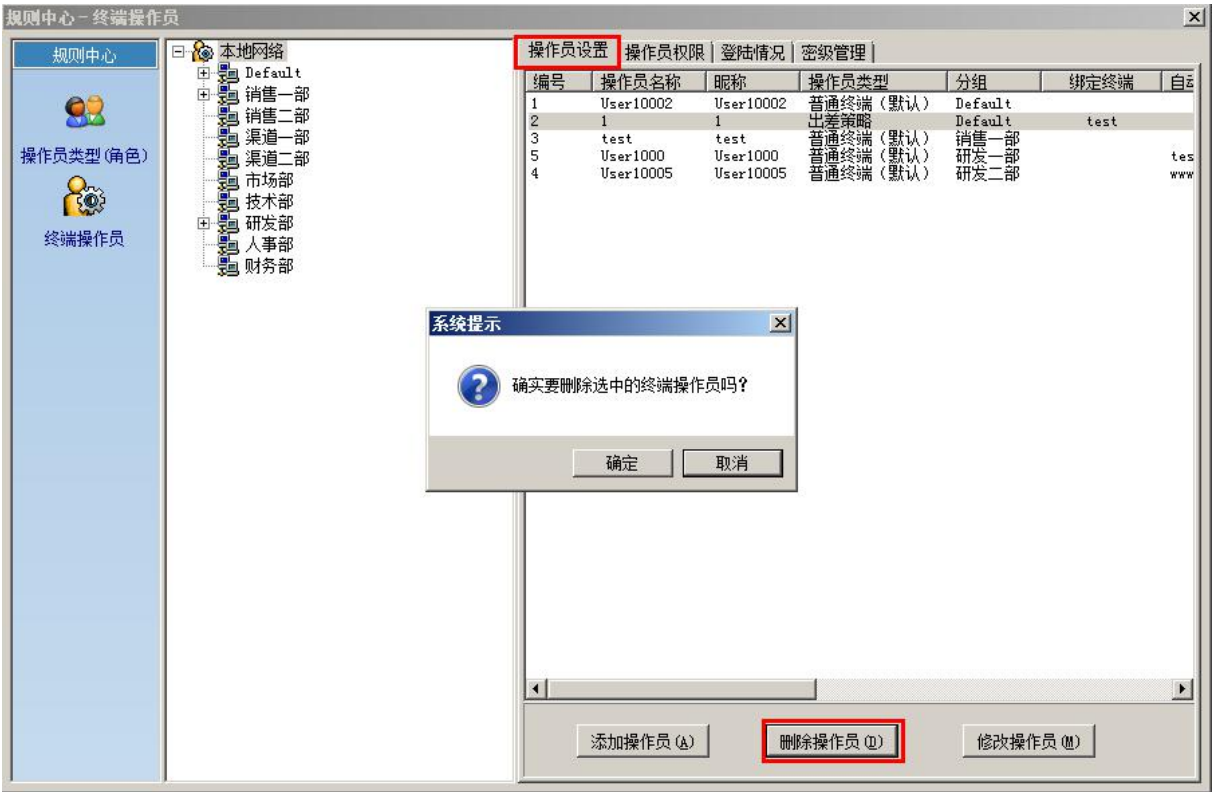
“同步终端所属分组为登陆的操作员分组”：对于在线的终端，可以同步其分组为登陆的操作员的所在分组。

“同步终端昵称为登陆的操作员昵称”：对于在线的终端，可以同步其昵称为登陆的操作员昵称。

同步方法是在“规则中心-终端操作员”窗口的左侧选中要同步的分组或操作员，再在窗口右侧右键鼠标，选择要同步的内容。如下图所示：



删除终端操作员：在“规则中心-终端操作员”窗口，在中间的“操作员列表”中选中需要删除的终端操作员，然后点击“删除操作员”按钮，在弹出确认对话框后点击“确定”即删除终端操作员成功。如下图所示：



2.1.5 操作员权限设置

设置分组或终端操作员只能阅读指定分组的加密文件。默认可以阅读整个公司的文件。在“规则中心-终端操作员”窗口，点击“操作员权限”页面选项，选中终端操作员，可以查看该终端操作员所拥有的文件阅读权限，可以删除或添加新的权限。

删除权限：选中要删除的权限，然后点击窗口右下方的“删除权限”按钮即可。

添加权限：选中终端操作员、分组或本地网络，然后点击窗口右下方的“添加权限”按钮，在弹出的“操作员权限”窗口中，勾选分组 A\B\C 并同时勾上“阅读文档”选项，点击“确定”，这样该终端操作员只能阅读指定分组 A\B\C 的文件。如下图所示：

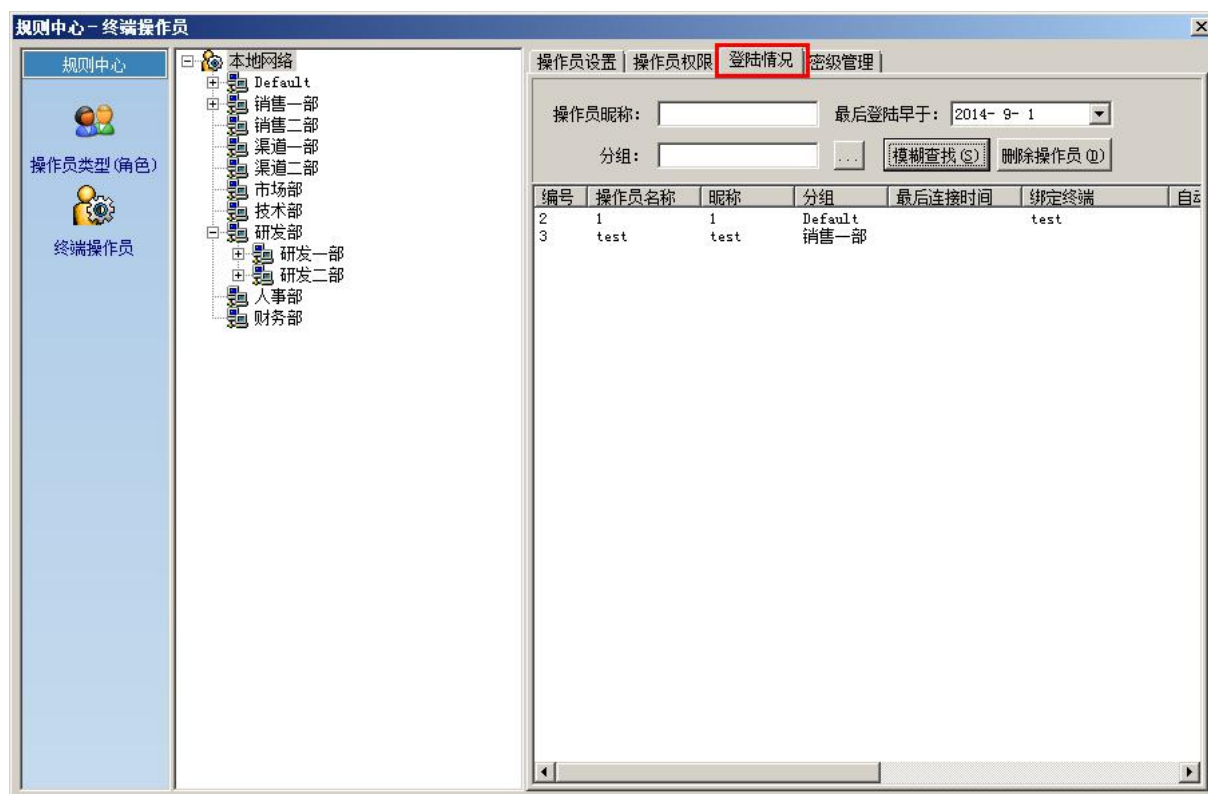


注意：在“操作员权限”中，每选中一个分组节点（以下简称节点）就可以设置一次“阅读文档”权限，当节点打勾且该节点对应的“阅读文档”复选框也打勾表示该终端操作员对该节点有阅读权限。“操作员权限”遵循继承原则，即当终端操作员对某节点的父节点有“阅读文档”权限，那么该终端操作员对该节点也有阅读权限。

2.1.6 登录情况

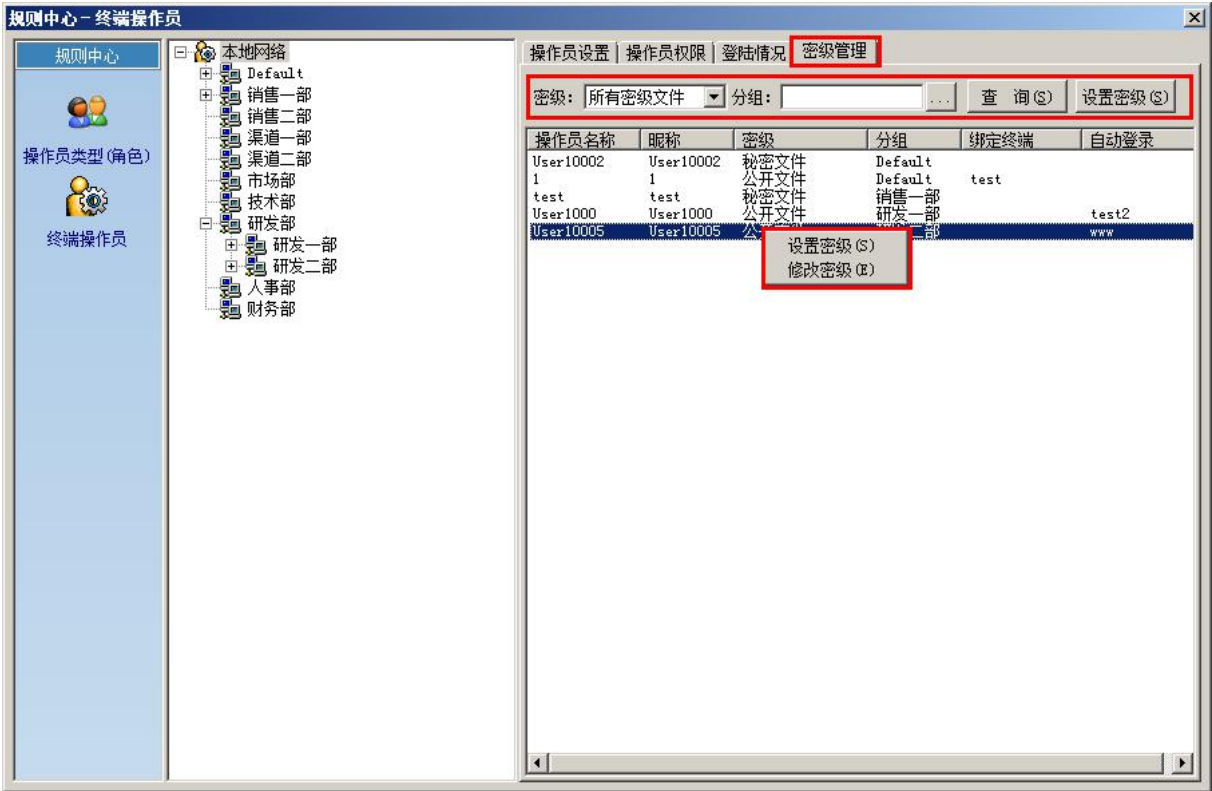
可以查看终端操作员的登录情况。在“规则中心-终端操作员”窗口，点击“登录情况”

页面选项，在窗口右侧输入要查询的操作员昵称或分组，选择“最后登录早于”的时间点，然后点击“模糊查询”按钮，即可列出最后登录早于指定时间的终端操作员。对那些长时间没登录、不用的终端操作员可以把它们删除，即选中不用的终端操作员，然后点击“删除操作员”按钮，也可以右键选中要删除的终端操作员，选择“删除操作员”，弹出询问窗口，确定即可。如下图所示：

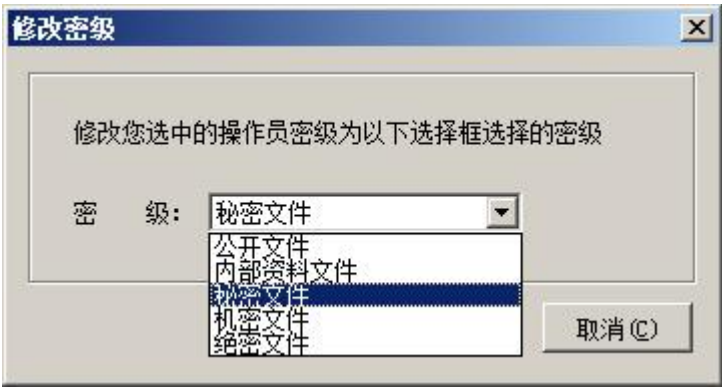


2.1.7 密级管理

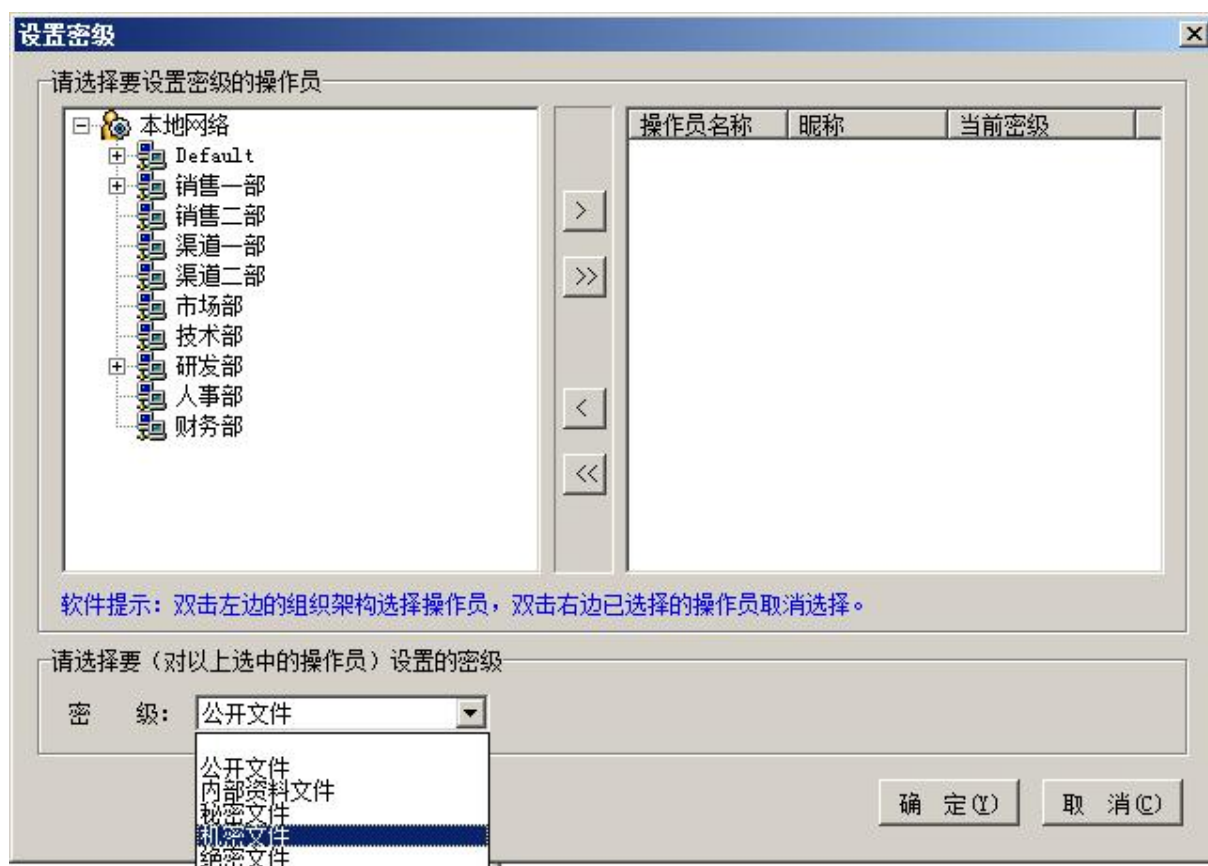
用户密级查询、修改，支持批量修改用户密级。在“规则中心-终端操作员”窗口，点击“密级管理”页面选项，选择要查询的用户密级、分组（分组默认为本地网络），然后点击“查询”，将列出符合条件的操作员及信息。如下图所示：



“修改密级”：修改指定操作员的用户密级。鼠标右键选中操作员，选择“修改密级”菜单，弹出“修改密级”窗口，如下图所示，在“密级”下拉框中选择要修改为的密级，再点击“确定”。



“设置密级”：批量设置或修改密级。点击“设置密级”按钮，或鼠标右键选择“设置密级”菜单，弹出“设置密级”窗口，如下图所示。先在窗口左侧选择要设置密级的操作员或分组，再点击窗口中间的“>”按钮，在窗口右侧将显示选择的操作员及其当前密级。在窗口底端的“密级”处选择要设置或修改为的密级，点击“确定”。

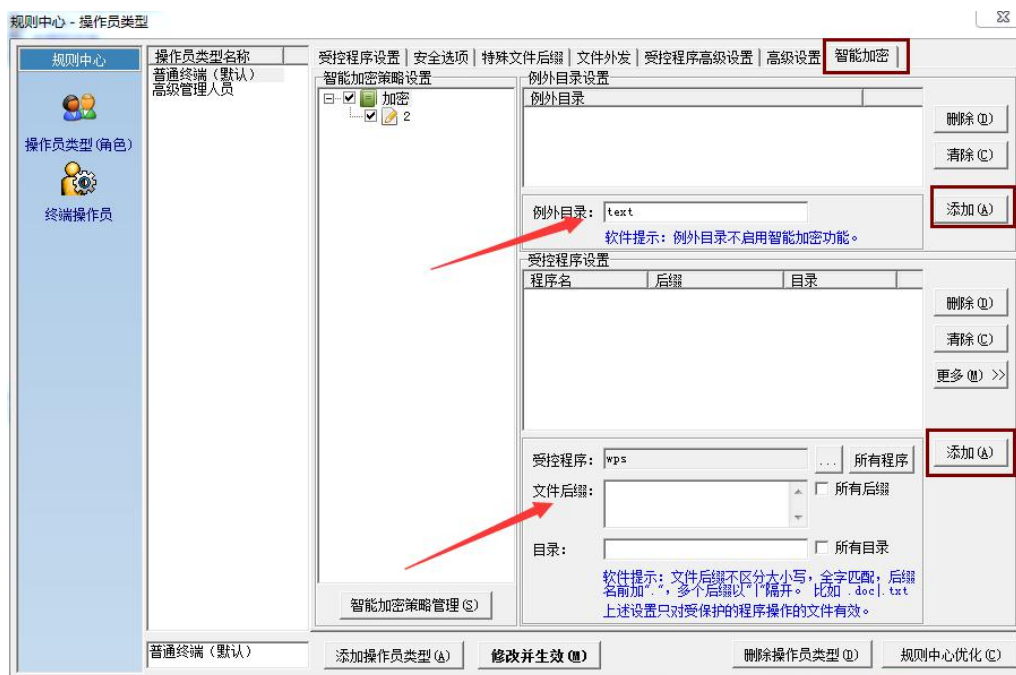


2.1.8 智能加密

在规则中心—操作员类型界面中，按住 **ctrl+alt+空白处左键** 调出智能加密功能。用户通过设置加密的关键字或正则表达式，扫描 office、PDF、纯文本文件是否包含指定关键词或正则表达式，包含则加密该文件，否则不加密。

“例外目录设置”：添加例外目录点击“添加”则该目录不启用智能加密功能。

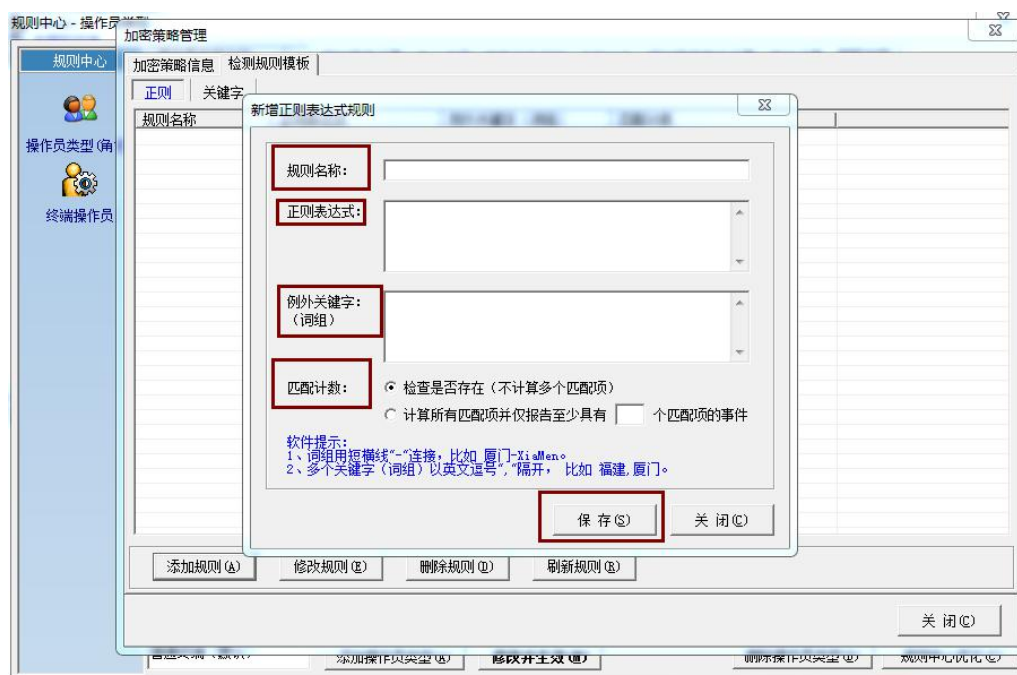
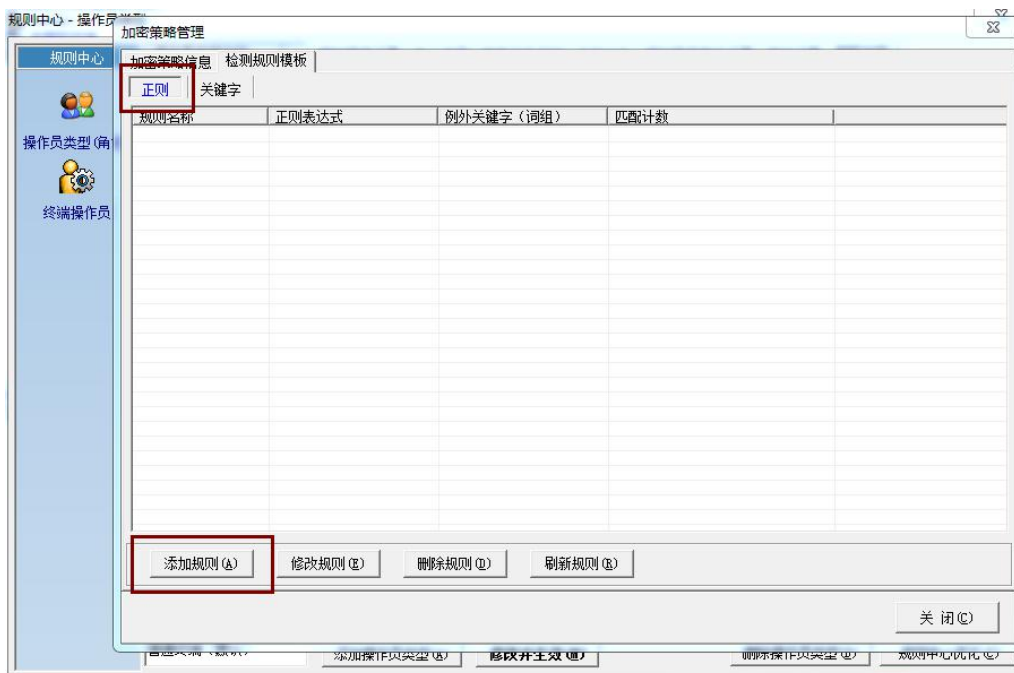
“受控程序设置”：添加受控程序，设置文件后缀、目录点击“添加”则该受控程序的文件进行智能加密。如下图所示。



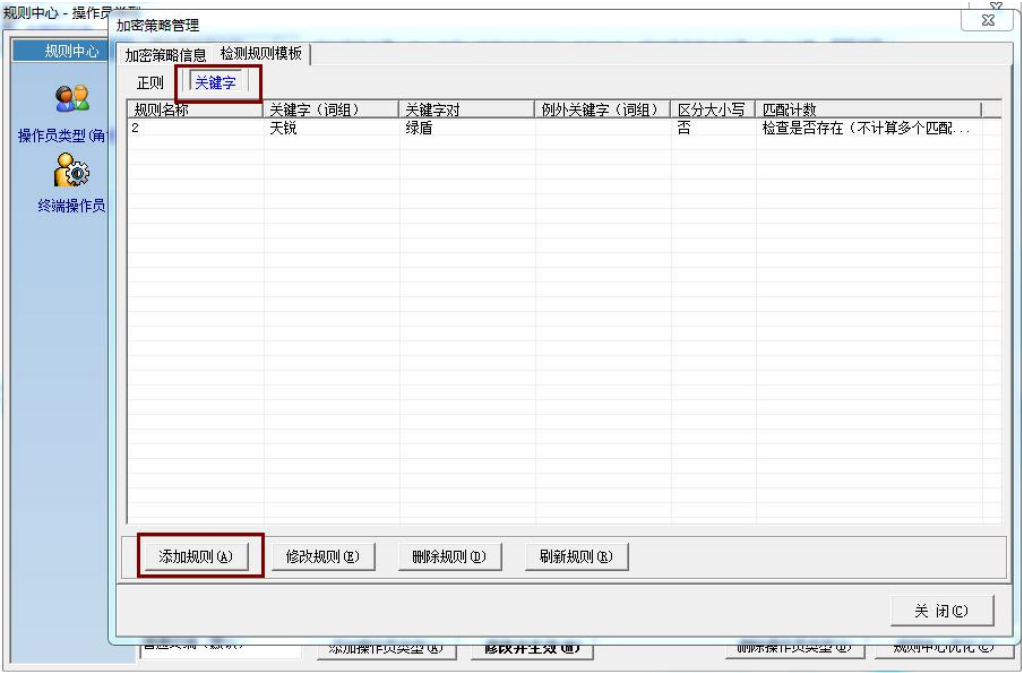
“智能加密策略管理”：设置智能加密的策略信息以及检测规则的模板。点击“智能加密策略管理”弹出“加密策略管理”界面，如下图所示，点击“检测规则模板”设置规则模板，主要通过两种方式：正则表达式、关键字。



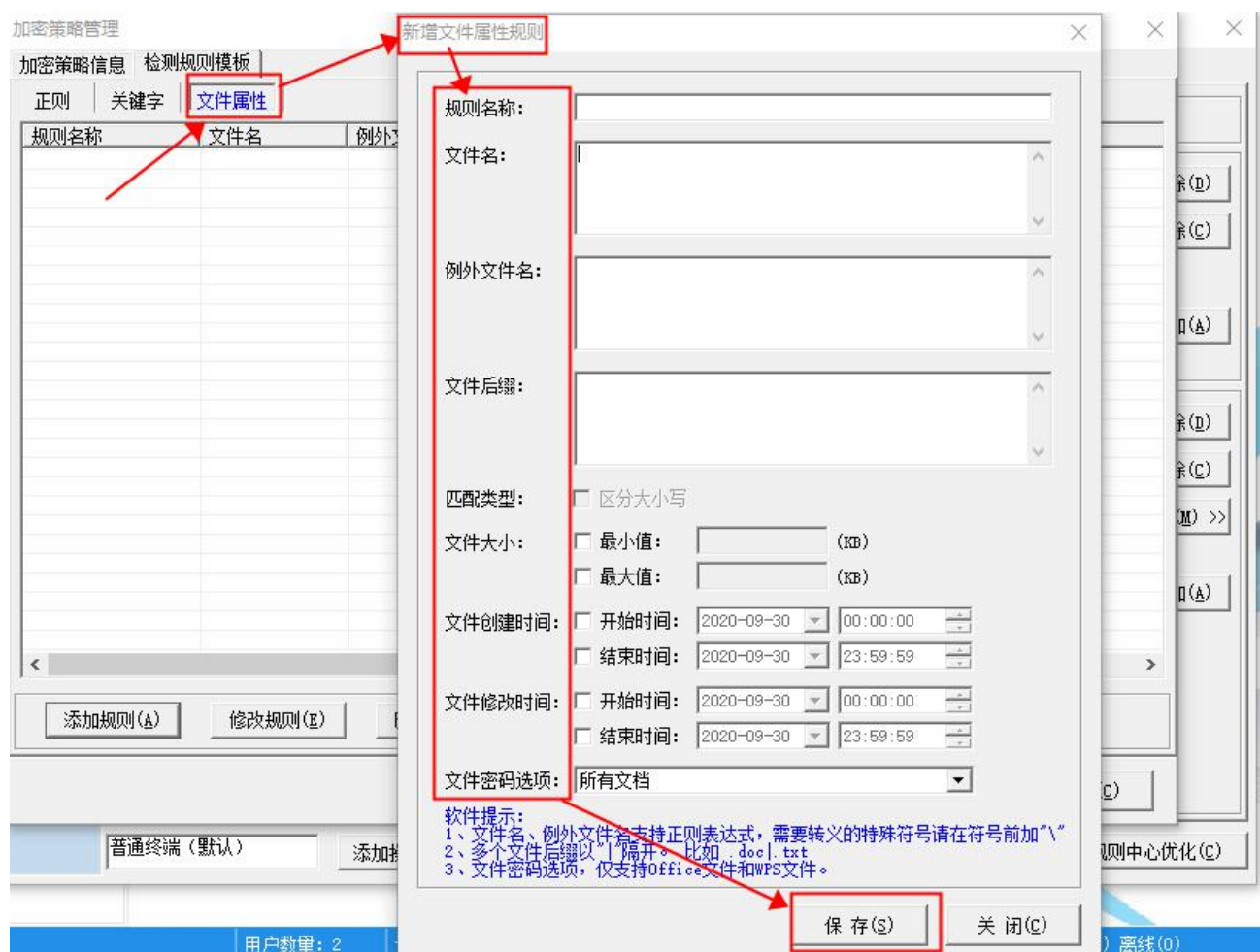
选择“正则”点击“添加规则”弹出“新增正则表达式规则”弹窗，设置相应的规则名称、正则表达式、例外关键词字（词组）、匹配计数，点击“保存”则该规则保存到列表中，如下图所示。选中某条规则点击“修改规则”或“删除规则”可对该规则进行修改和删除。



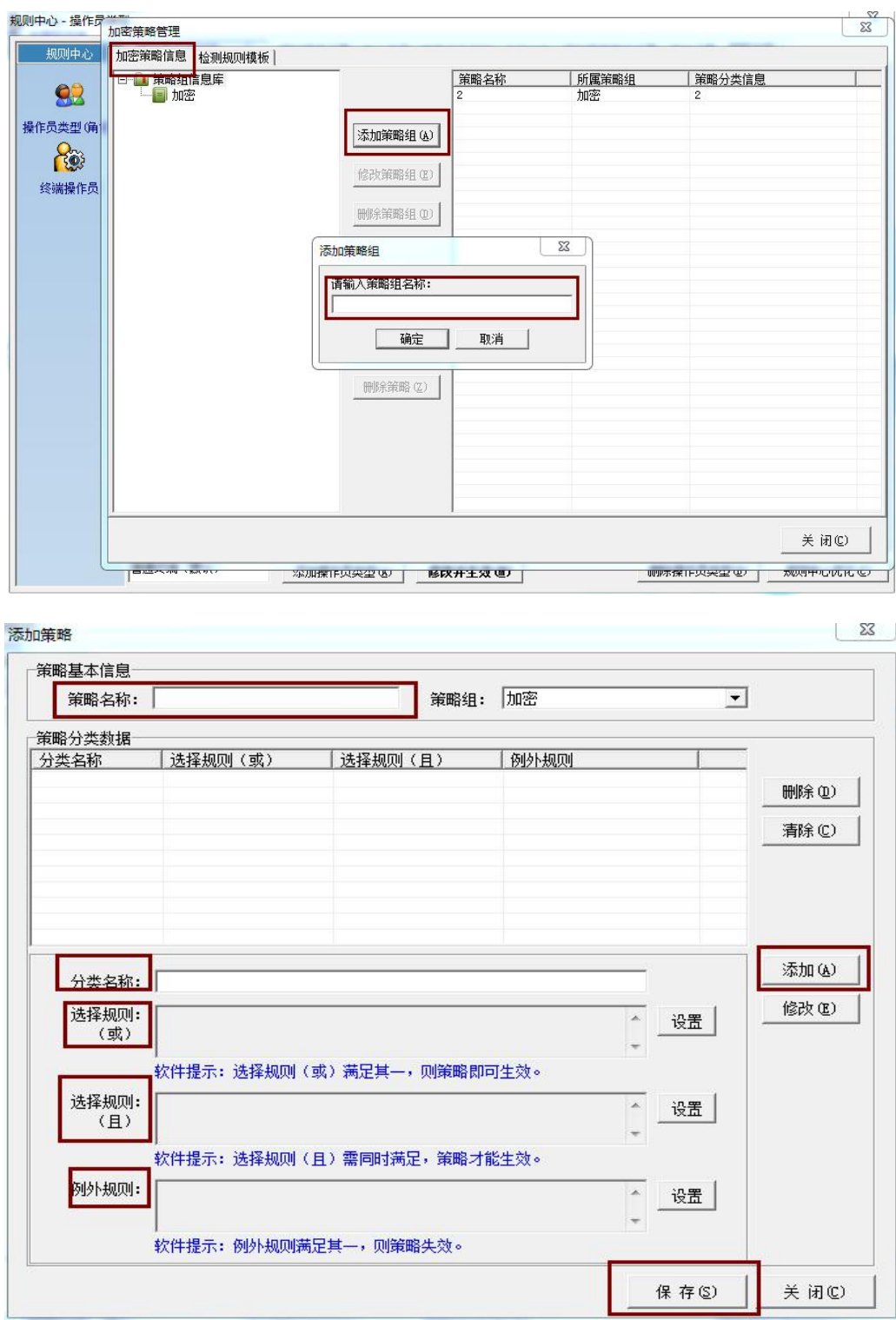
选择“关键字”点击“添加规则”弹出“新增关键字规则弹窗”，设置相应的规则名称、关键字（词组）、邻近关键字对、例外关键字（词组）、匹配类型、匹配计数，点击“保存”则该规则保存到列表中，如下图所示。选中某条规则点击“修改规则”或“删除规则”可对该规则进行修改和删除。



选择“文件属性”点击“添加规则”弹出“新增文件属性规则”弹窗，设置相应的规则名称、文件名、例外文件名、文件后缀、匹配类型、文件大小、文件创建时间、文件修改时间文件密码选项，点击“保存”则该规则保存到列表中，如下图所示。选中某条规则点击“修改规则”或“删除规则”可对该规则进行修改和删除。



点击“加密策略信息”进入策略信息列表，点击“添加策略组”弹出策略组名称添加弹窗，设置策略组名称点击确定，如下图所示。选中策略组点击“添加策略”弹出“添加策略”弹窗，设置策略名称、分类名称、选择规则（或）、选择规则（与）、例外规则，点击“添加”则该规则添加到策略分类数据表中，选中某条策略可对该策略进行删除、修改。点击“保存”则该策略保存到策略管理列表中。



2.2 企业密钥

文件加密密钥由三部分组成：主密钥、企业密钥和文件密钥。

主密钥：自动生成，由厦门天锐分配给每个客户全球唯一的密钥；

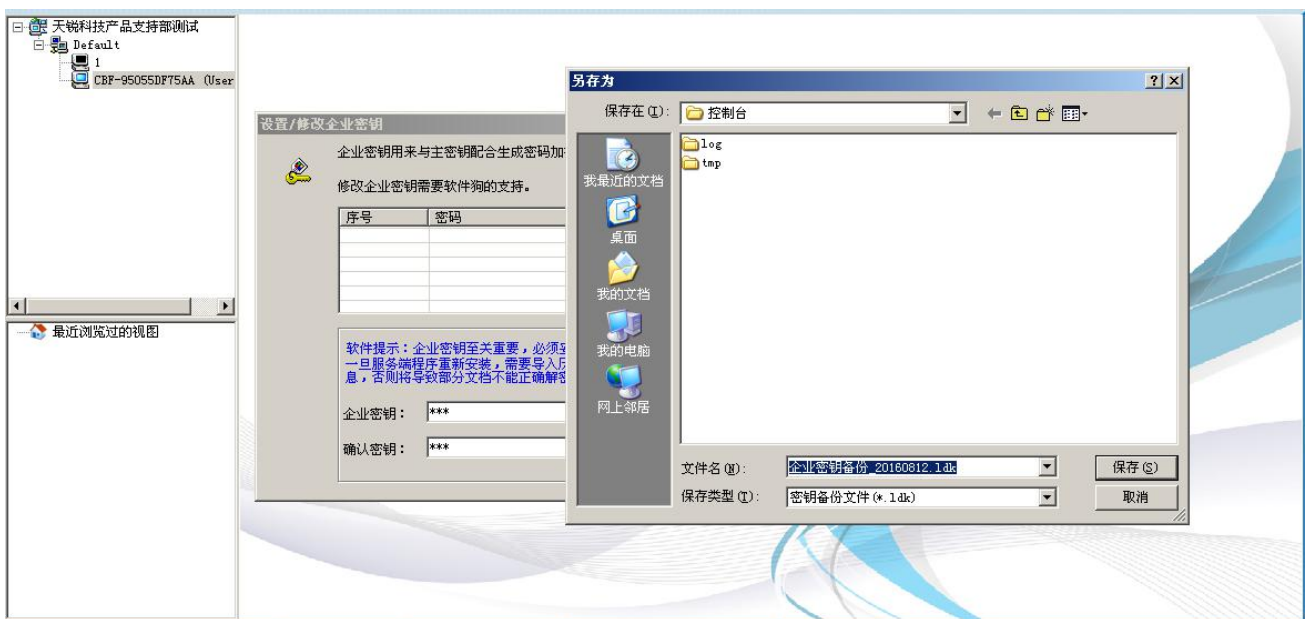
企业密钥：由客户自行设置，可以修改，若序列号丢失或被他人获取的情况下，他人可以新搭建天锐绿盾服务端，如果没有得到相应的企业密钥，也是无法对加密的文件进行解密；

文件密钥：每个文件加密时会随机生成一个文件密钥，以提高加密的安全性。

2.2.1 设置/修改企业密钥

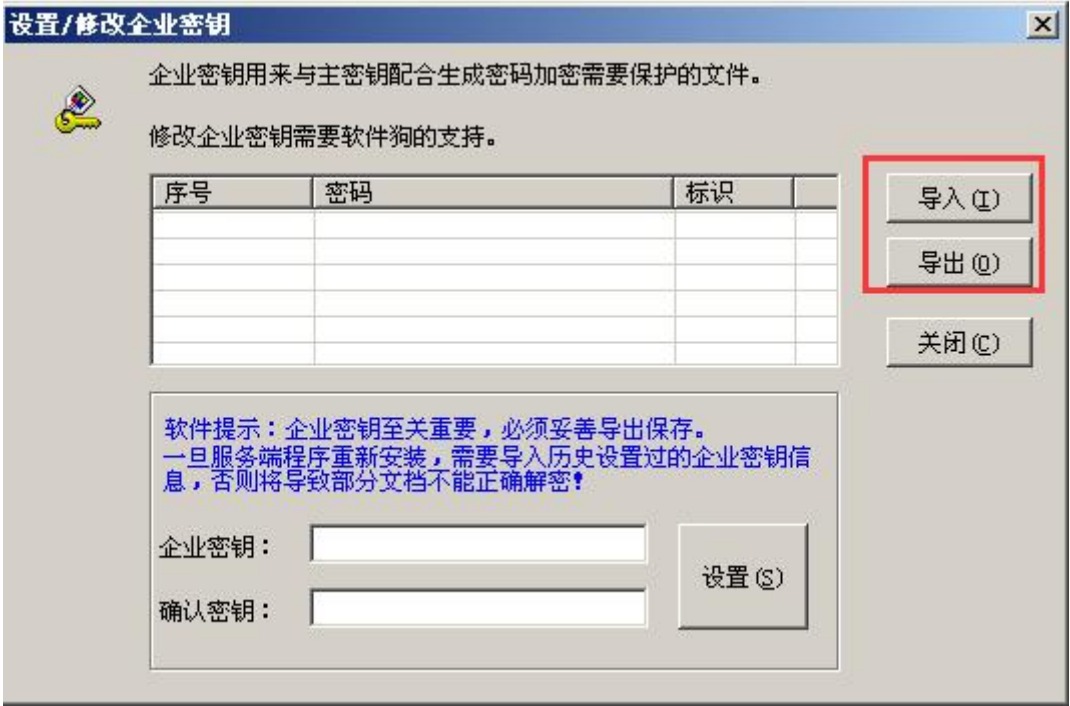
正式客户修改企业密钥需要有软件狗的支持（类似 U 盘的存储设备），而试用用户只能设置一次企业密钥并且无法进行修改。

在控制台的功能列表选择“文件加密”-“企业密钥”，将弹出“设置/修改企业密钥”窗口，在“企业密钥”和“确认密钥”中输入需要设置或者修改的企业密钥。设置企业密钥后，系统会自动弹出导出备份企业密钥窗口，保存企业密钥。如下图所示：



2.2.2 导入/导出企业密钥

企业密钥的设置/修改支持导入、导出功能，即可将设置好的企业密钥导出备份，这样当系统或软件重装后可方便地导入原来设置的企业密钥，有效防止因企业密钥丢失而导致加密文件无法打开的故障。在“设置/修改企业密钥”窗口，如果已经设置好企业密钥，可单击“导出”按钮，选择备份路径保存企业密钥。导入企业密钥则单击“导入”按钮，然后找到已备份好的企业密钥后导入即可。如下图所示：



2.3 密级设置

可以根据企业特殊要求设置密级级别、描述和图标样式。

在控制台的功能栏选择“文件加密”-“密级设置”，弹出“密级设置”窗口，可以设置启用密级数（最高 4 级），修改密级、密级描述和图标样式。设置完成点击“保存”即可。如下图所示：



2.4 离线策略

如果公司有笔记本电脑安装了天锐绿盾终端，当操作员需要将电脑带回家工作或者出差时，天锐绿盾终端脱离了天锐绿盾服务端，打开加密文件就会显示为密文（乱码），导致无法正常使用加密文件。为此，天锐绿盾提供了离线策略功能，即在离线策略时间内终端还可以正常使用加密文件。

注意：在离线策略时间内，终端电脑上的加密文件拷贝到其他没有安装终端或没有权限的电脑上仍然保持加密状态，不能查看。在离线策略时间内，终端不能申请解密，终端的操作记录会暂时保存在本地，当与服务器再次通信时上传到服务器。

离线策略适用于终端电脑需要较长时间脱离公司网络的情况，通常为非日常使用，如带笔记本电脑出差的情况。如果碰到出差时间延长等情况，可以由管理员在公司内部再制作一个相应时间的离线策略发给该员工，然后重新导入新的离线策略即可。

在控制台的功能栏选择“文件加密”-“离线策略”，在弹出的“生成离线策略文件”窗口中设置“绑定终端”、“保护”、“有效期”、“文件名”（生成的文件路径）后点击右下角的“确定”按钮即可以生成离线策略文件。如下图所示：



“绑定终端”：包含“所有终端均可使用”、“只适用于指定分组的终端”（表示生成的离线策略文件只能在指定分组的终端上导入）和“只适用于指定终端上使用”（表示生成的离线策略文件只能在指定的终端电脑上导入）；

“有效期”：包含“开始时间”和“结束时间”，即该离线策略文件的时效（导入该离线策略的终端电脑可以脱离天锐绿盾服务端的工作时长），最长可设置为 180 天；

“保护”：可以设置“导入时需要输入密码”，即终端用户导入该离线策略文件时需要输入密码方可导入；

“导入离线策略后启动全盘加密”：导入离线策略后，终端执行全盘加密任务操作。配置详见本文档的“全盘加解密”部分。**请慎用该功能，不要把系统目录以及程序安装目录进行加密，导致系统/程序运行不了。**



“文件名”：该离线策略文件保存的路径和文件名，点击文本框右边的“...”按钮可设置保存该离线策略文件的路径和名称。

其他设置

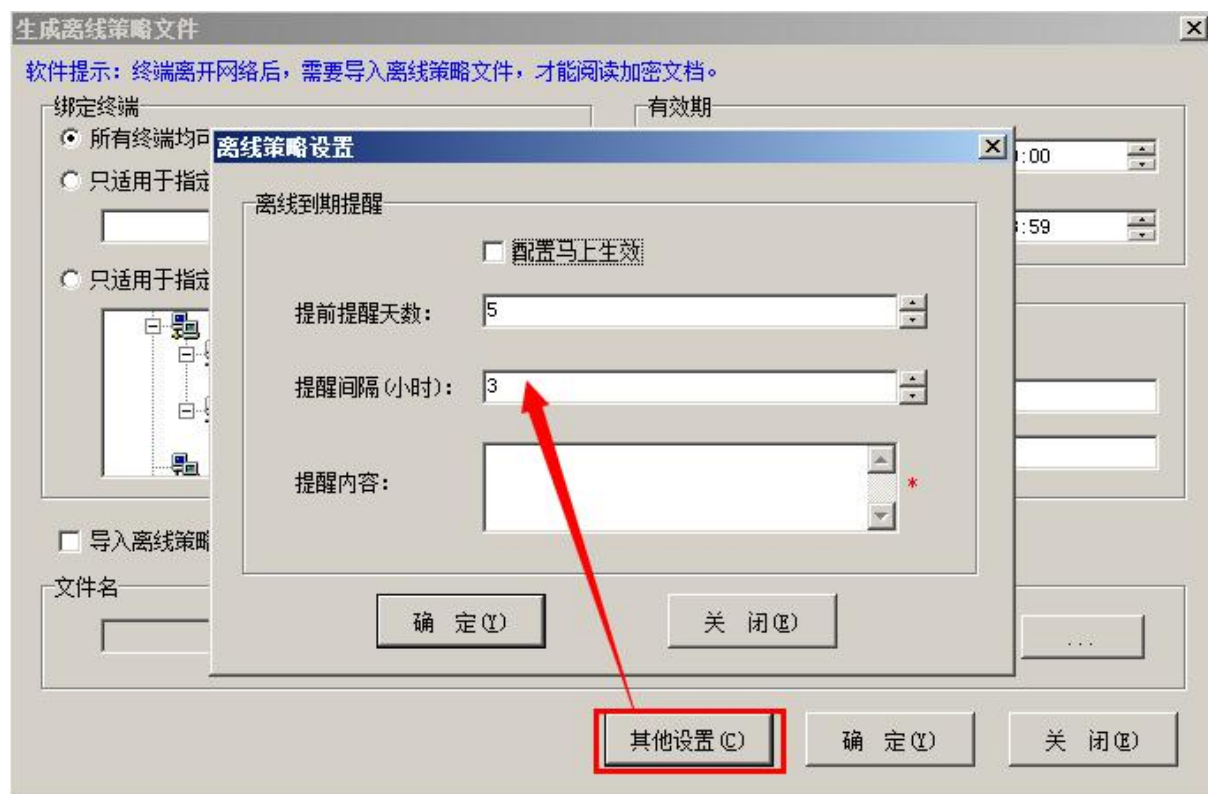
在其他设置里，可以设置离线到期提醒信息，各设置选项说明如下：

“配置马上生效”：勾选该选项，离线到期提醒设置才会生效；

“提前提醒天数”：距离离线到期前 X（设置的天数）天时，开始提醒；

“提醒间隔（小时）”：每隔 Y（设置的时间间隔）小时提醒一次，如果是一天提醒一次，则填写 24 小时；

“提醒内容”：提醒时需要显示的内容。



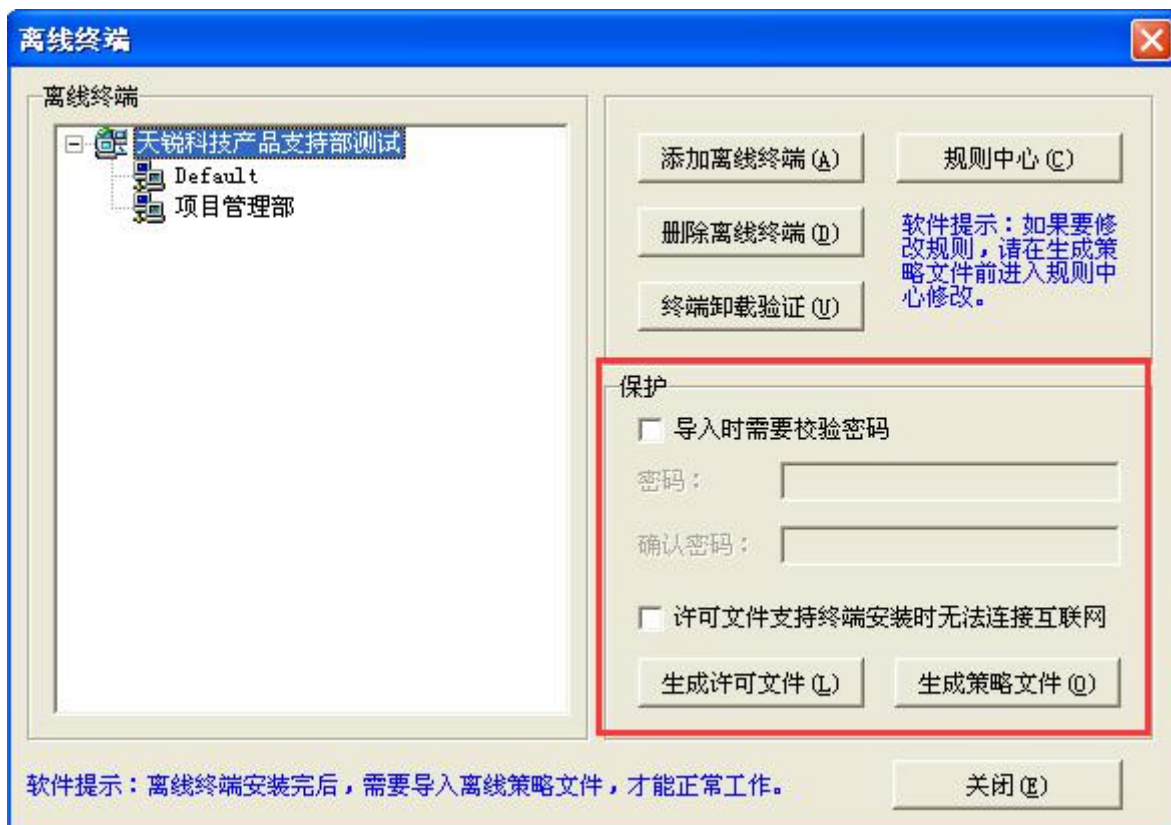
2.5 离线终端

有些电脑需要长期脱离公司网络，但也需要保护电脑上的文件，同时，需要查看公司其他电脑上的加密文件，这时，可以选择在这类电脑上安装离线终端。

在控制台的功能栏选择“文件加密 - 离线终端”，弹出“离线终端”窗口。在窗口左侧的分组架构列表中选择某个分组，然后单击“添加离线终端”按钮，在弹出的“请输入离线终端名称”窗口中输入要添加的离线终端名称，确定。添加离线终端时，控制台电脑要求能够联网。添加成功将在该分组下新增一个离线终端节点。如下图所示：

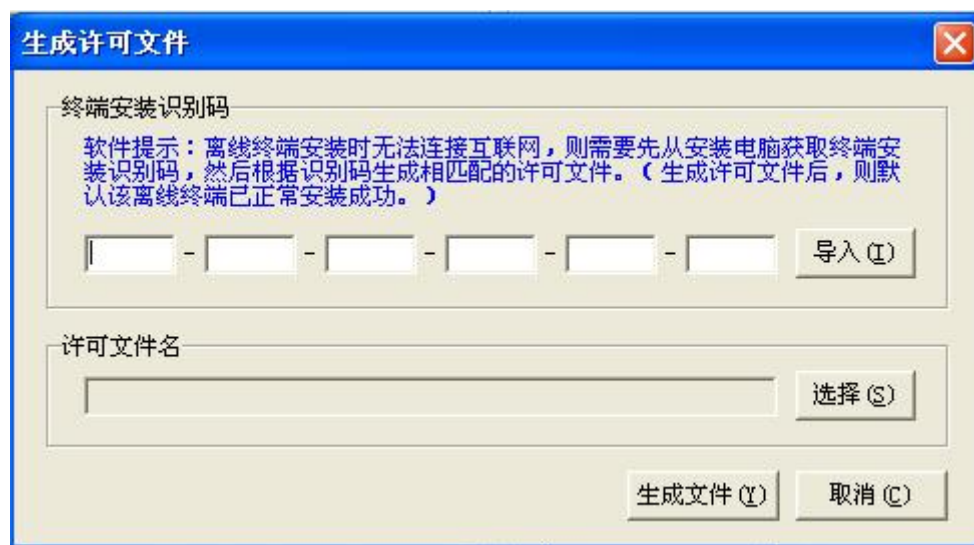


在“离线终端”窗口，点击“规则中心”按钮，可自动链接打开“规则中心”窗口，可以添加离线终端操作员等配置。配置定义完成就可以生成安装该离线终端的许可文件和策略文件。在“离线终端”窗口左侧选中刚才创建好的离线终端，如下图所示：



在“保护”里可以选择设置导入时是否需要输入密码，如果终端电脑断网安装离线终端的

话请勾选“许可文件支持终端安装时无法连接互联网”，然后点击“生成许可文件”按钮，将会弹出“生成许可文件”，需要先输入终端安装识别码，如下图所示：



然后选择文件存放路径，设置完成后点击“生成文件”则生成扩展名为.lsf 的离线安装许可文件。点击“生成策略文件”按钮，生成扩展名为.lof 的离线策略文件。将这两个文件发给目标计算机进行安装。

说明：

1. 如果控制台电脑不能联网，可以联系天锐股份技术人员处理生成授权文件，然后进行相关配置。
2. 终端识别码获取:请将运行离线终端安装程序时获取到的终端识别码发送给管理员生成许可文件。

2.6 全盘加解密

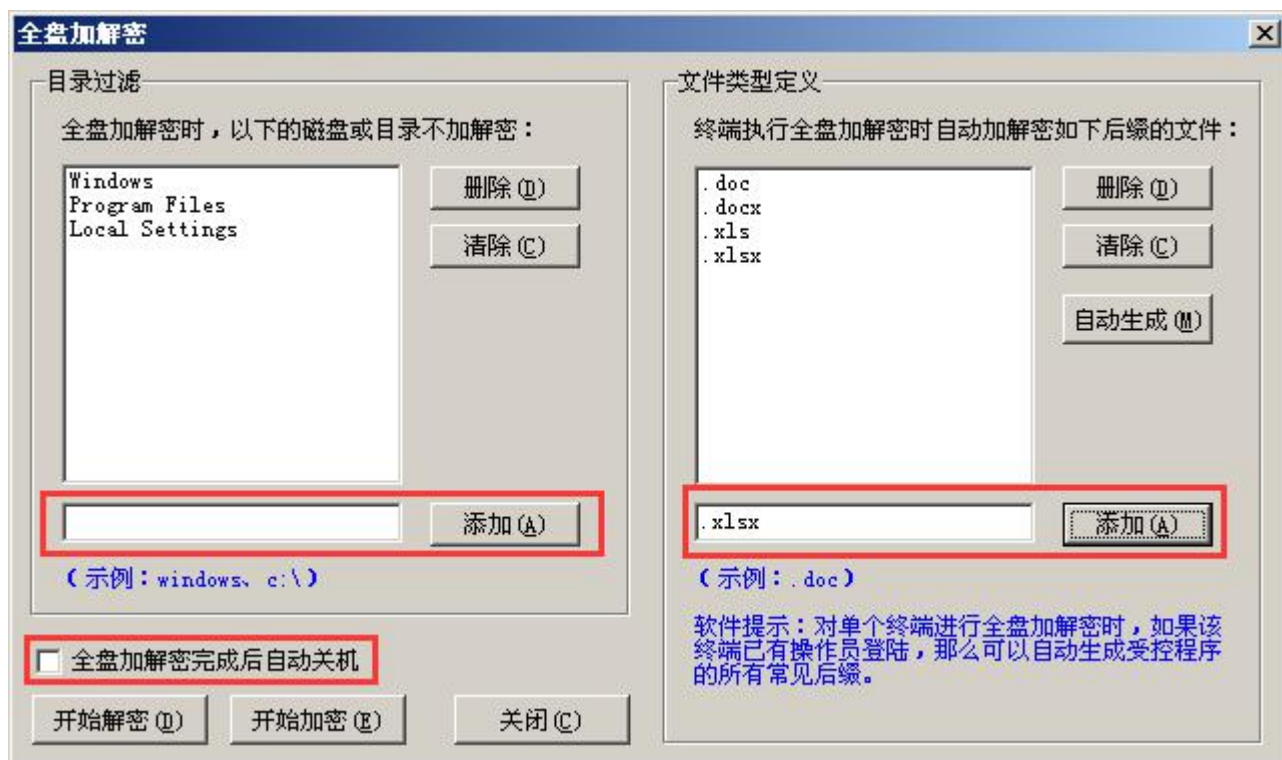
天锐绿盾对操作编辑过的文档进行加密，在安装天锐绿盾之前创建的文档是未加密的。安装天锐绿盾后，可通过“全盘加密”功能将 Windows、Mac 终端电脑上的指定类型的文档加密。

但是要慎用，不要把系统目录以及程序安装目录进行加密，导致系统/程序运行不了。

在卸载天锐绿盾终端程序之前需要先把终端电脑上的加密文件进行解密，可以通过控制台上的“全盘加解密”功能进行全盘解密。此外，全盘加密或解密操作完成后可以设置终端电脑自动关机。

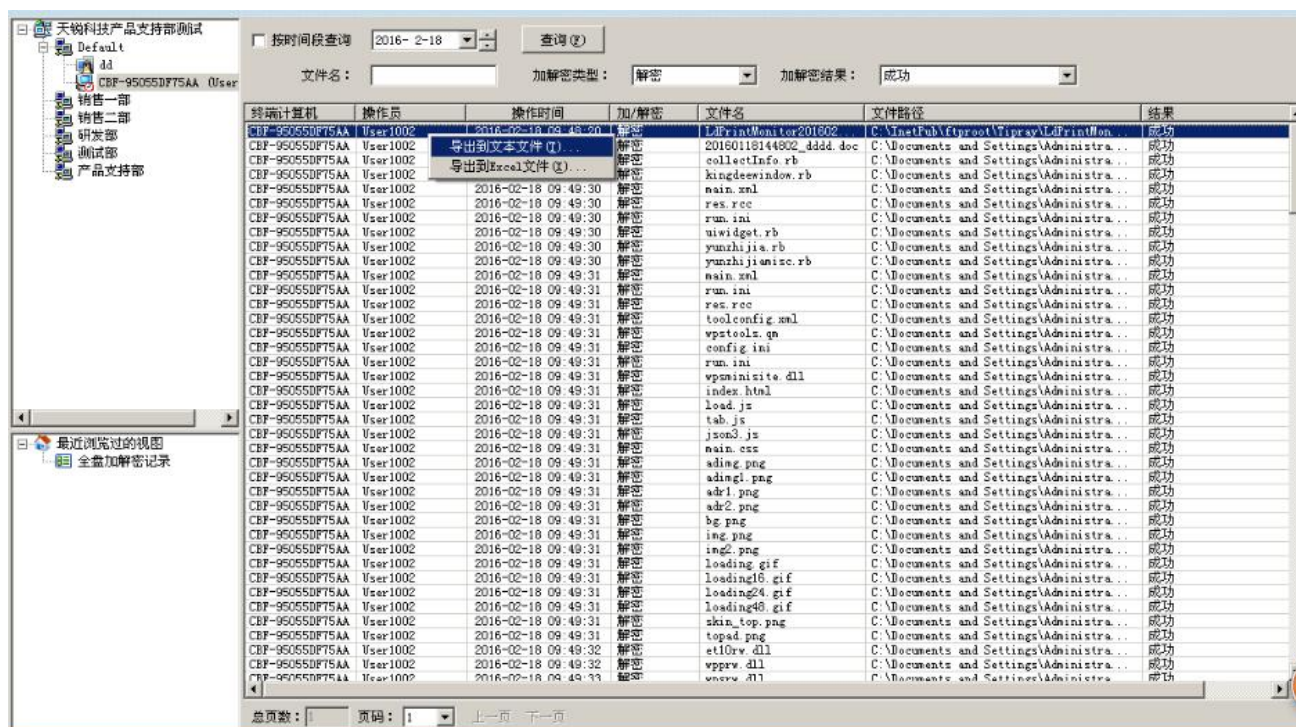
用户列表栏选择要全盘加解密的终端，然后在控制台的功能栏选择“文件加密”-“全盘加解密”，弹出“全盘加解密”窗口（也可直接右键选中需要全盘加解密的终端-远程控制-全盘加解密），在窗口右侧的“文件类型定义”的文本框中输入需要加密的文件类型（如.doc），并点击“添加”按键（可多次添加文件类型）。窗口左侧的“目录过滤”表示全盘加解密时指

定目录下的文件不进行加解密，可根据需要在“目录过滤”的文本框中输入需要过滤的目录名称，并点击“添加”按键来添加需要过滤的目录。全盘加解密操作完成后可以设置终端电脑自动关机，即勾选“全盘加解密完成后自动关机”选项。设置完成后点击“开始加密”或者“开始解密”即可。如下图所示：



2.7 全盘加解密记录

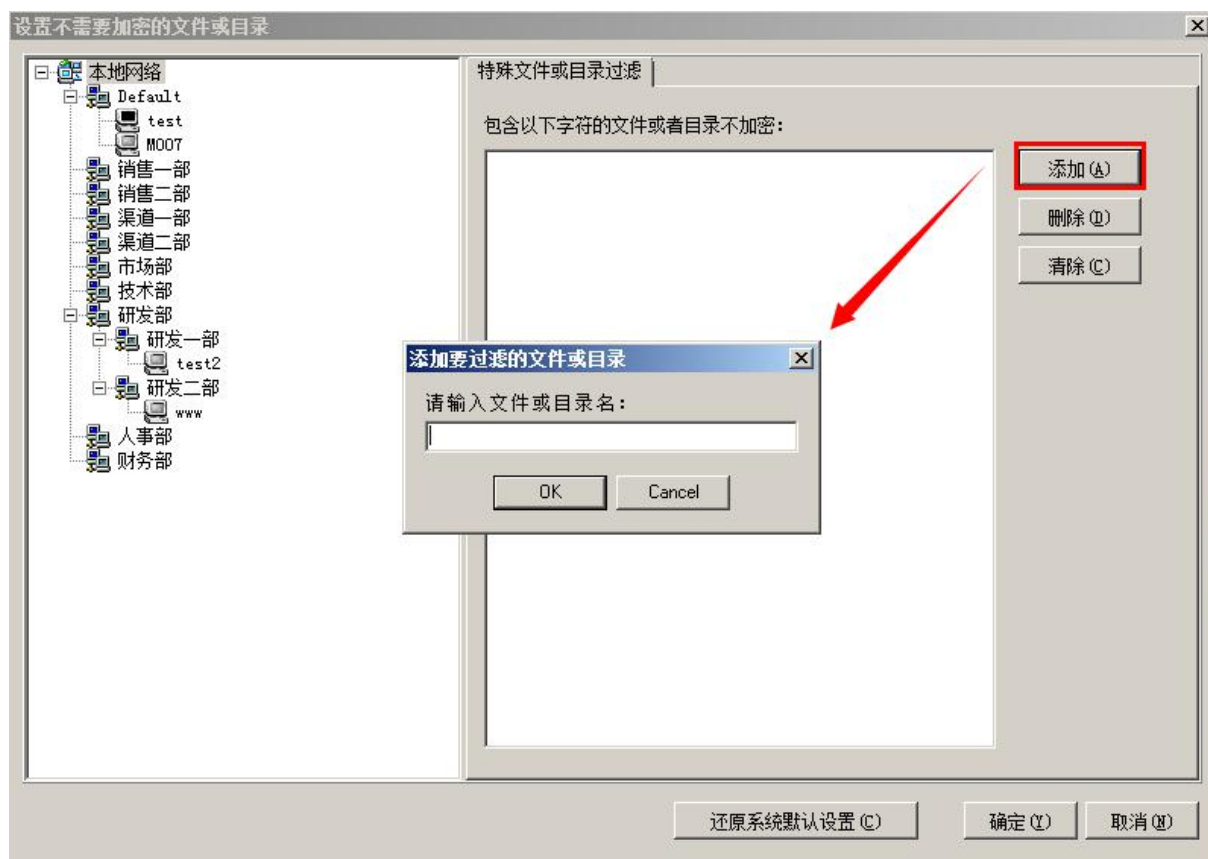
在控制台的功能栏选择“文件加密”-“全盘加解密记录”，用户列表栏选择要查看的对象（可以选择本地网络、分组或终端），在详细信息栏将显示选中用户进行全盘加解密操作的情况。全盘加解密记录信息包括：终端计算机、操作员、操作时间、加/解密、文件名、文件路径和结果。如下图所示：



2.8 特殊目录设置

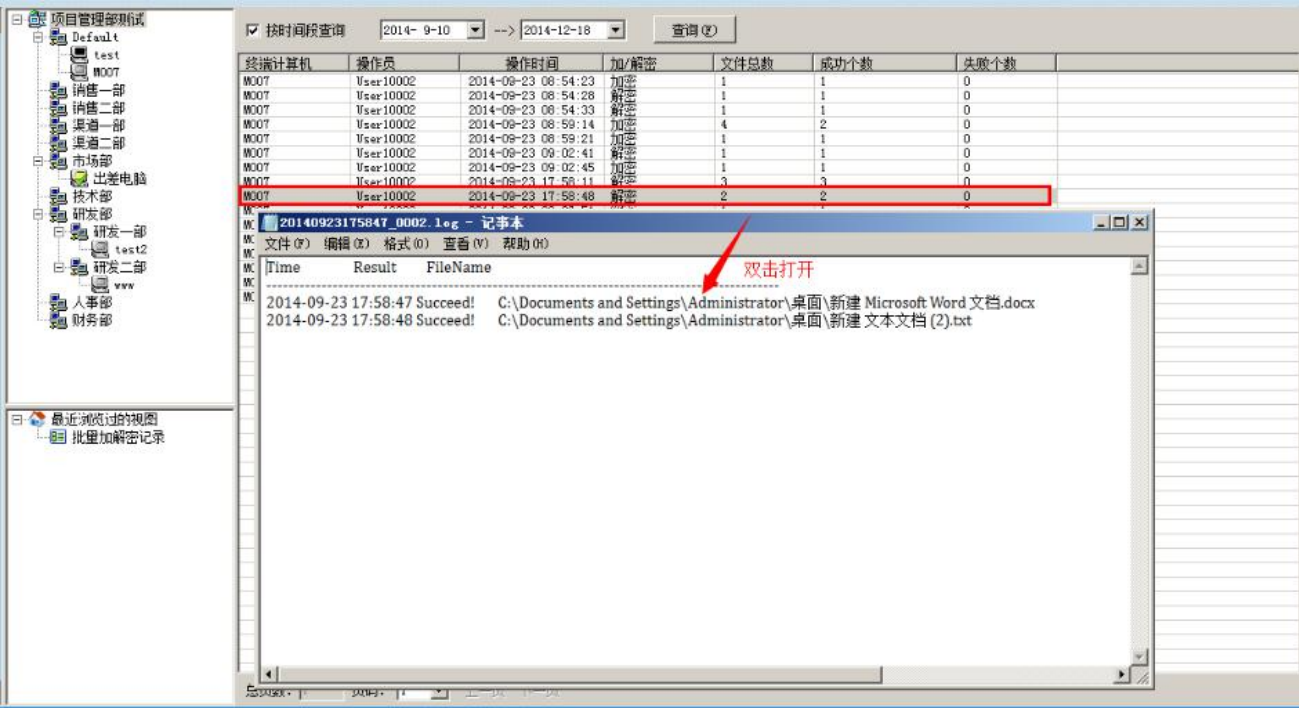
特殊目录可以设置指定终端的某个目录或某个文件不进行加密（包含指定字符的文件或目录不加密）。

在控制台的功能栏选择“文件加密”-“特殊目录设置”，在弹出的“设置不需要加密的文件或目录”窗口左侧选择需要设置的终端或分组，在窗口右侧点击“添加”按钮，输入特殊文件或目录名称即可。如果要删除特殊目录，先选择要删除的特殊目录，然后点击“删除”即可。如图所示：



2.9 批量加解密记录

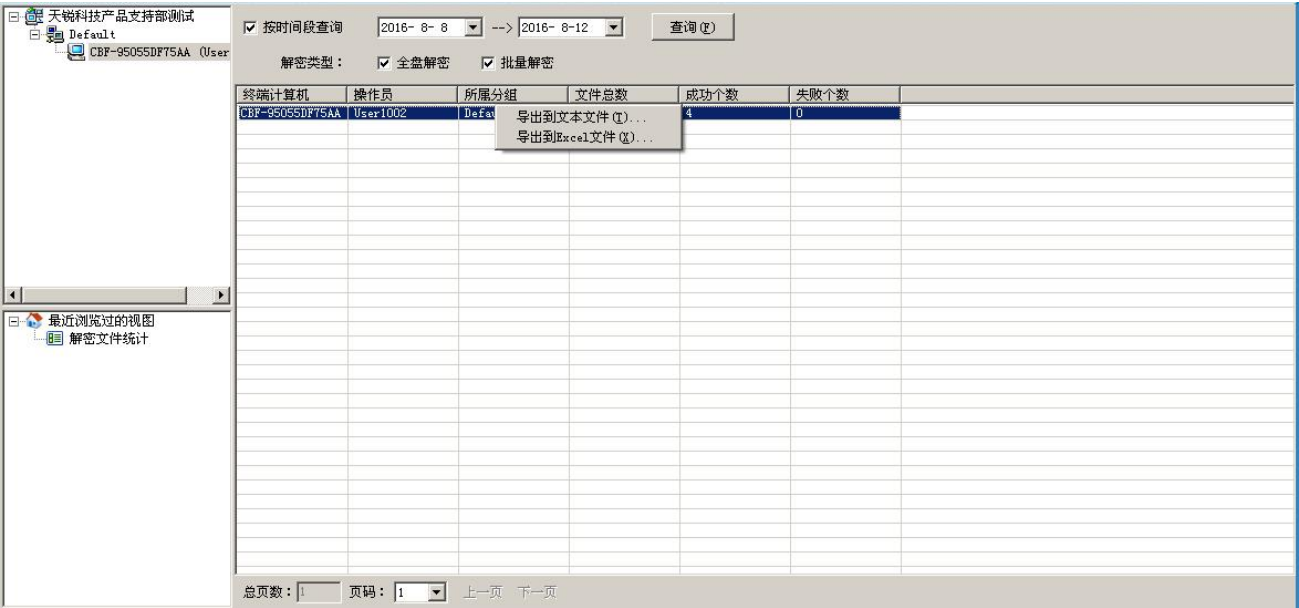
在控制台的功能栏选择“文件加密”-“批量加解密记录”，用户列表栏选择要查看的对象（可以选择本地网络、分组或终端），在详细信息栏将显示选中用户进行批量加解密操作的情况。批量加解密记录信息包括：终端计算机、操作员、操作时间、加/解密、文件名、文件路径和结果。如下图所示：



2.10 解密文件统计

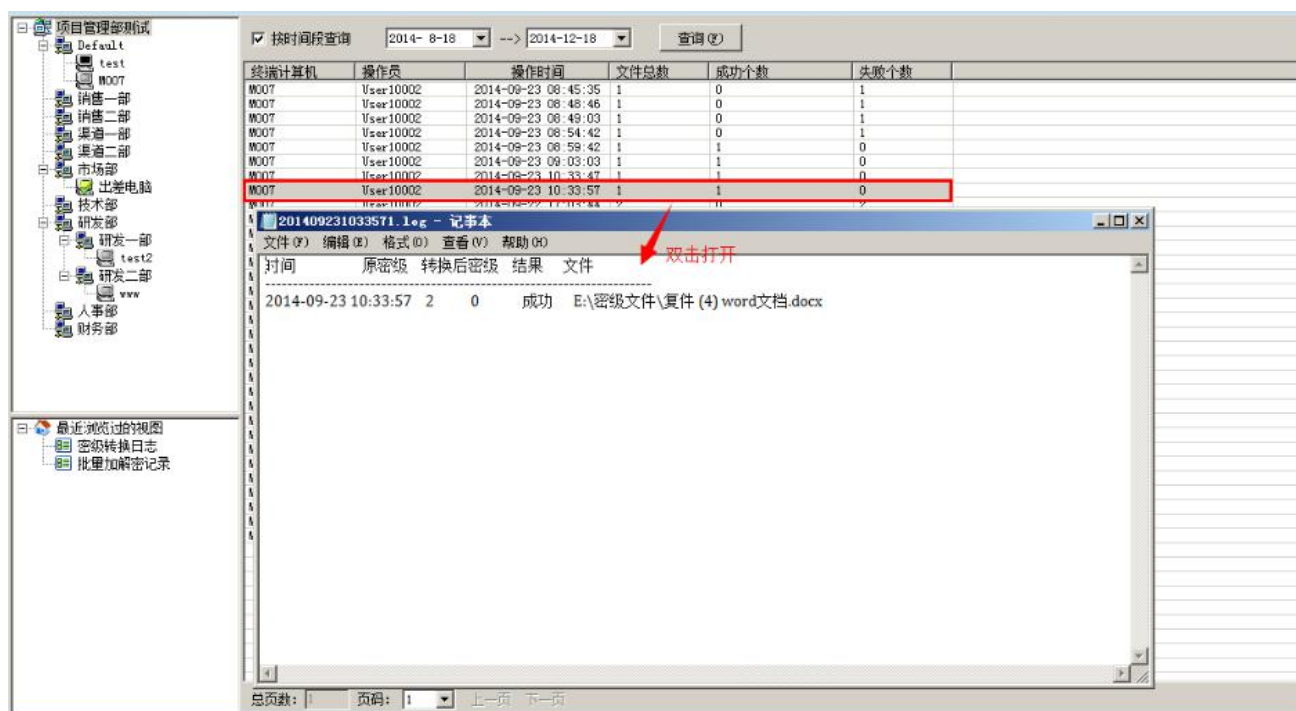
可以统计全盘加密文件和批量解密文件的个数。

在控制台的功能栏选择“文件加密”-“解密文件统计”，用户列表栏选择要查看的对象（可以选择本地网络、分组或终端），在详细信息栏将显示选中用户解密文件的统计情况。解密文件统计信息包括：终端计算机、操作员、所属分组、文件总数、成功个数和失败个数。如下图所示：



2.11 密级转换日志

在控制台的功能栏选择“文件加密”-“密级转换日志”，用户列表栏选择要查看的对象（可以选择本地网络、分组或终端），在详细信息栏将显示选中用户进行文件密级转换的日志记录。记录信息包括：终端计算机、操作员、操作时间、文件总数、成功个数、失败个数。双击记录，可以查看详细情况，包括时间、原密级、转换后密级、结果和文件路径。如下图所示：



2.12 文件备份记录

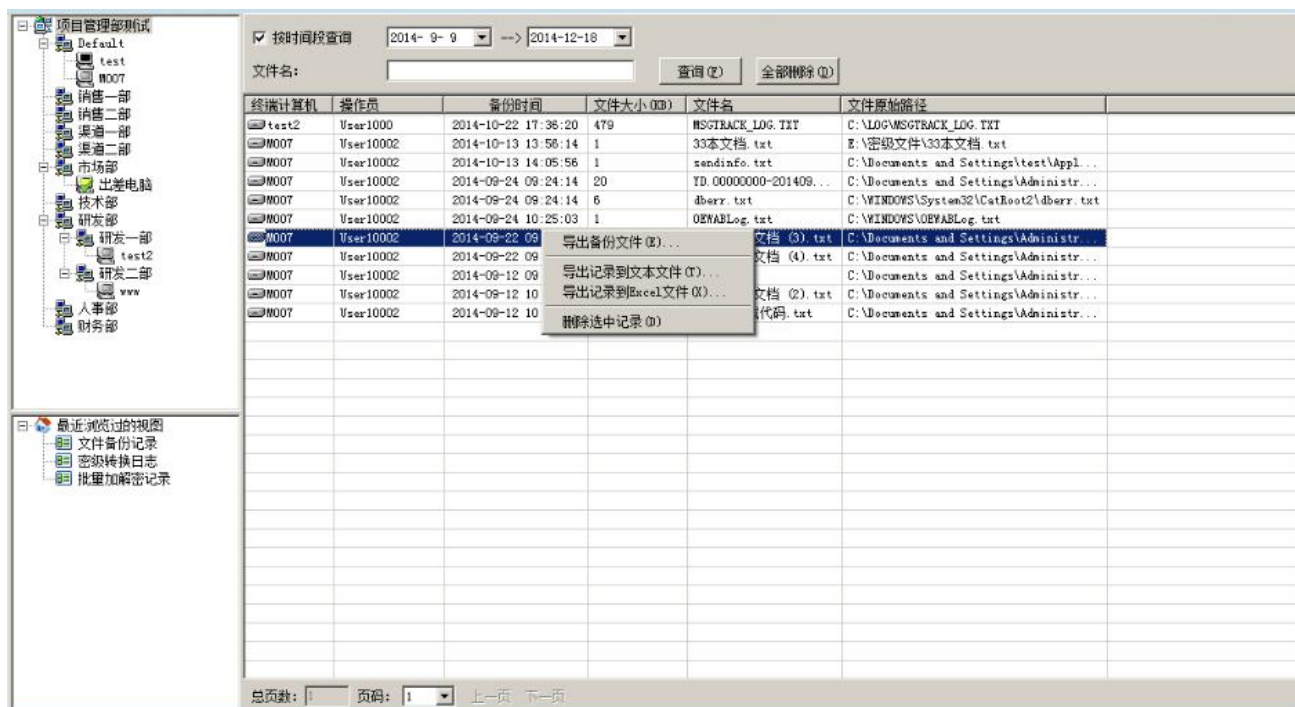
文件备份功能主要是避免重要文件遭破坏或恶意删除等情况而设置的，终端电脑的文件备份情况可以从控制台的文件备份记录中查看。

注意：备份的文件是以天锐绿盾终端上的文件路径为标志，即终端电脑上不同路径下保存的同名文件在服务器上均有备份（在不同终端上的同名文件也有分别备份）。

2.12.1 查看文件备份记录

在控制台的功能栏选择“文件加密”-“文件备份记录”，在用户列表栏选中要查看的用户（可以选择本地网络、分组或终端），详细信息栏将显示选中用户当天的文件备份情况。备份记录信息包括：终端计算机、操作员（申请外发的终端用户）、备份时间、文件大小（KB）、

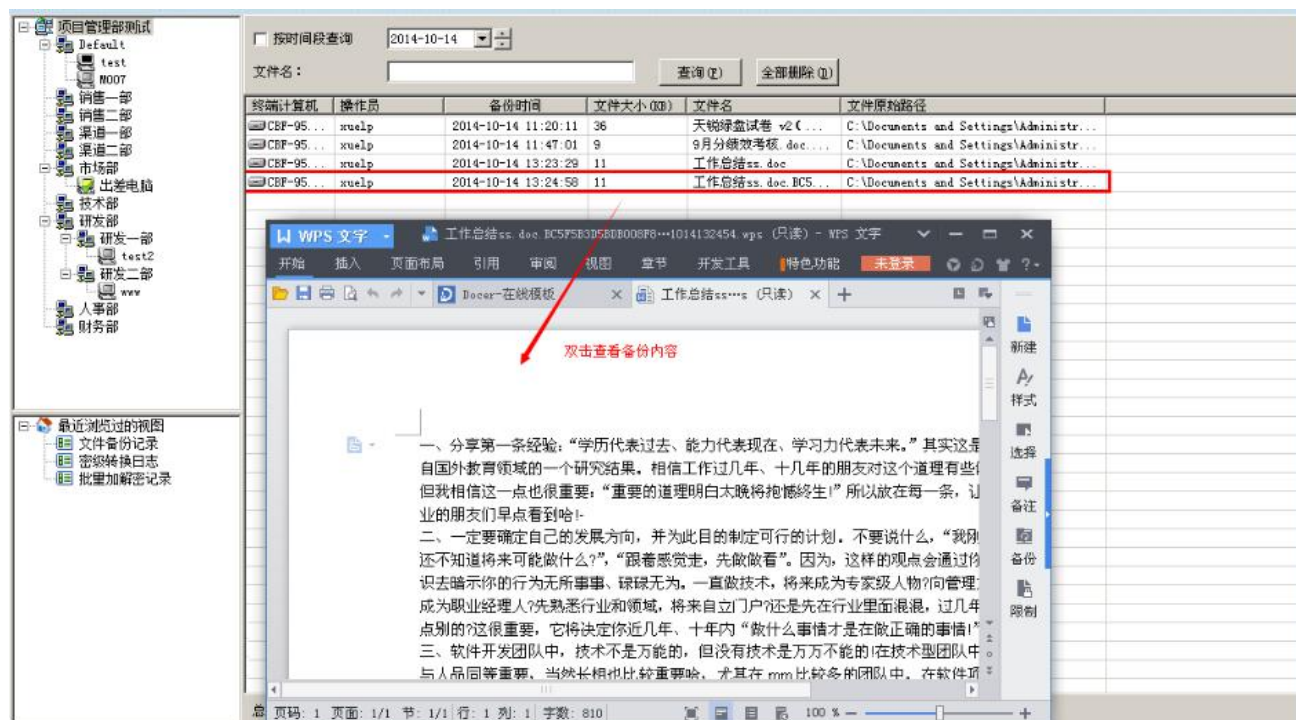
文件名、文件原始路径。可选择按某一具体时间或时间段查询文件备份记录：选择要查询的日期（打勾“按时间段查询”则可以按时间段查询备份记录），点击“查询”按钮即可查询对应时间的文件备份记录，也可以根据文件名查询指定的备份记录。如下图所示：



2.12.2 查看备份文件内容

管理员可以根据需要查看天锐绿盾服务端所备份文件的具体内容。

查询出指定终端的备份文件记录后,在文件备份记录列表中选中需要查看文件内容的备份记录,双击即可打开该备份文件并查看该文件内容,也可以右键导出备份文件。如下图所示。



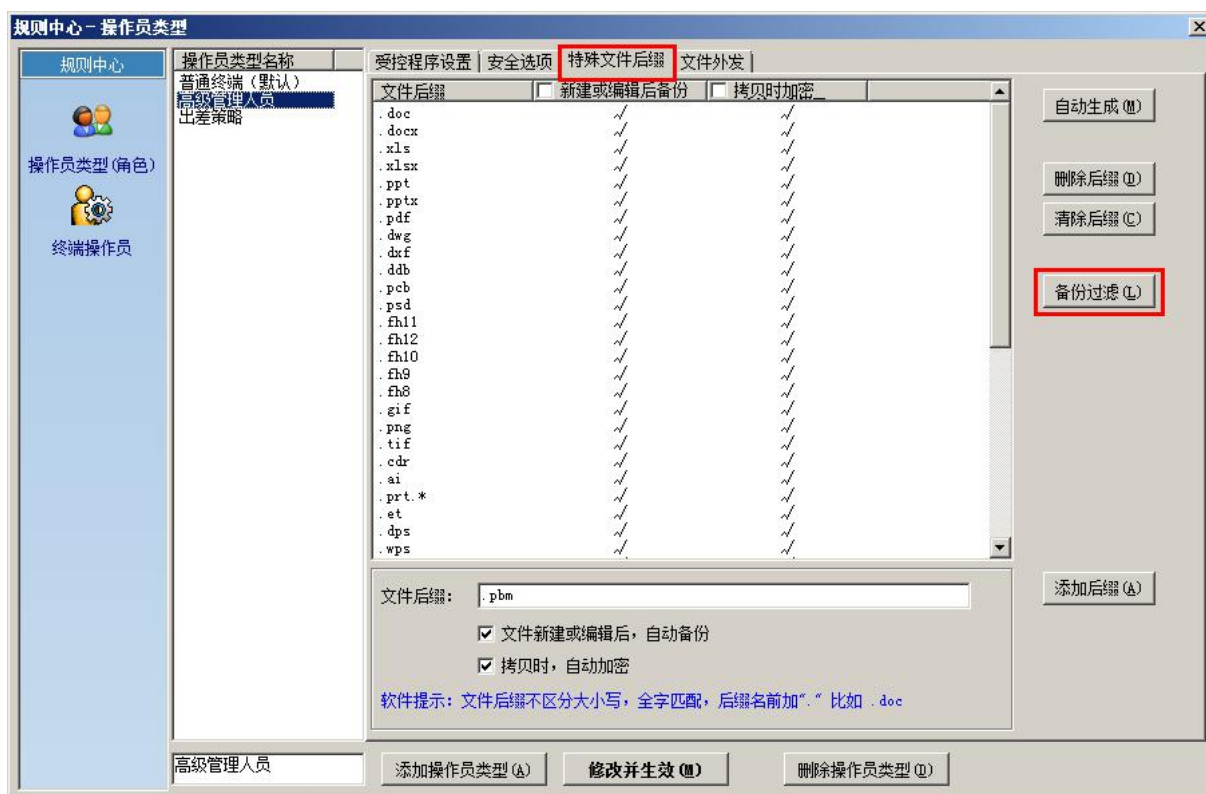
2.12.3 过滤不需要的文件类型备份

管理员可以根据需要设置不需要备份的文档类型。

在控制台的功能栏选择“文件加密”-“规则中心”，在“规则中心-操作员类型”窗口的操作员类型名称栏选中要设置的操作员类型，点击“特殊文件后缀”页面选项，然后在“特殊文件后缀”界面中点击“备份过滤”按钮，弹出“设置备份过滤”窗口。备份过滤可按目录名、进程名和文件大小来进行设置，只要满足这三个条件之一的文件就不会备份，如下图所示。

如果所有文件都不备份，在“特殊文件后缀”窗口中把所有文件后缀的“新建或编辑后备份”项的“√”去掉（鼠标单击“√”处即可），或者直接在“过滤设置”中勾选“关闭文件自动备份功能”。

说明：若点击“清除后缀”按钮，拷贝时自动加密功能也将去除。



备注: 备份过滤可按目录名、进程名和文件大小来进行设置, 只要满足这三个条件之一的文件就不会备份。

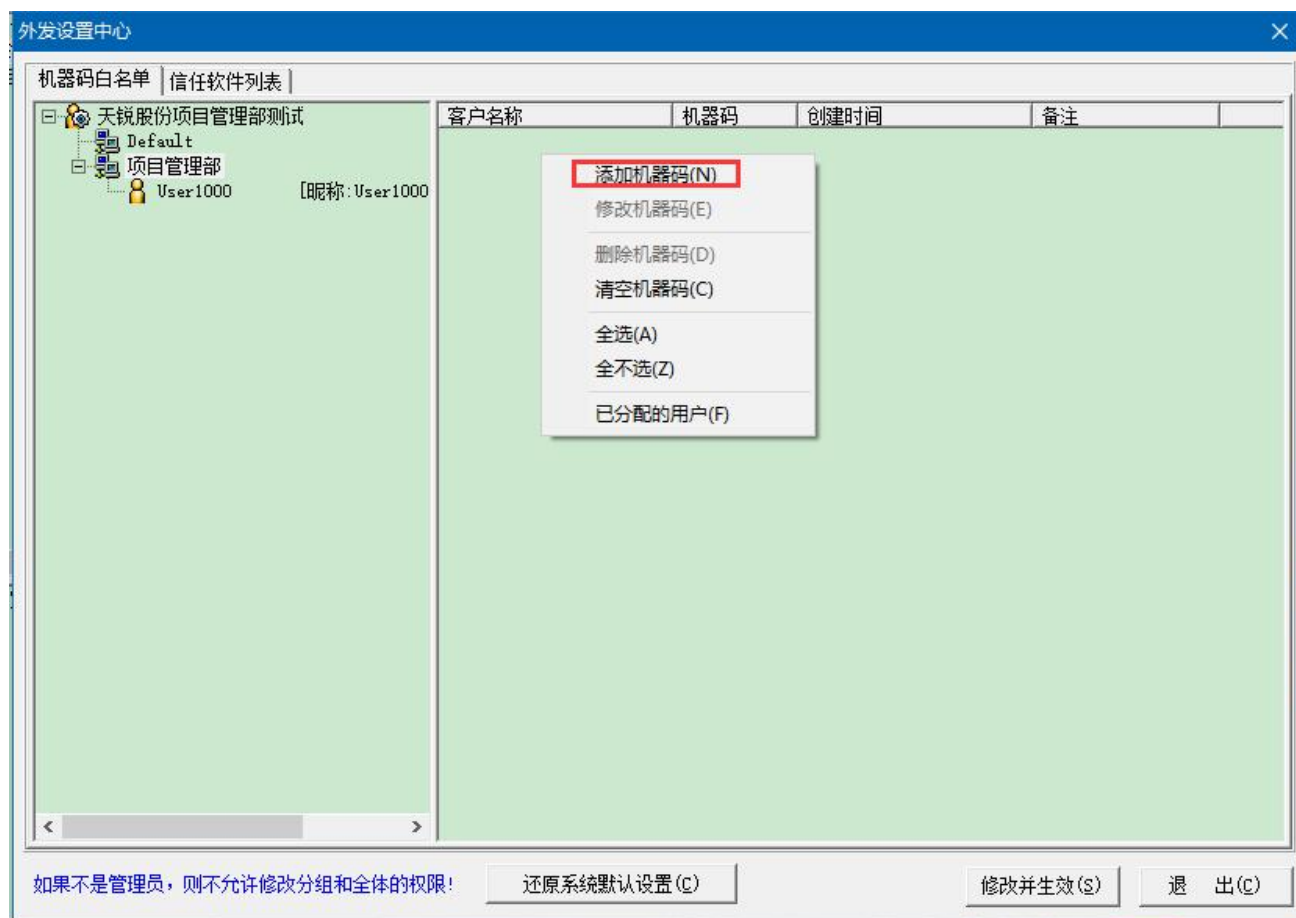
2.13 外发设置中心

2.13.1 机器码白名单

可以把一些经常往来的合作单位计算机机器码添加到“外发机器码白名单”，终端用户在制作直接外发文件的时候，就可以把指定的机器码内置到外发文件中，这些白名单计算机在打开外发文件的时候就不用验证机器码就能直接打开文件，而其他计算机仍需要验证机器码后才能打开。

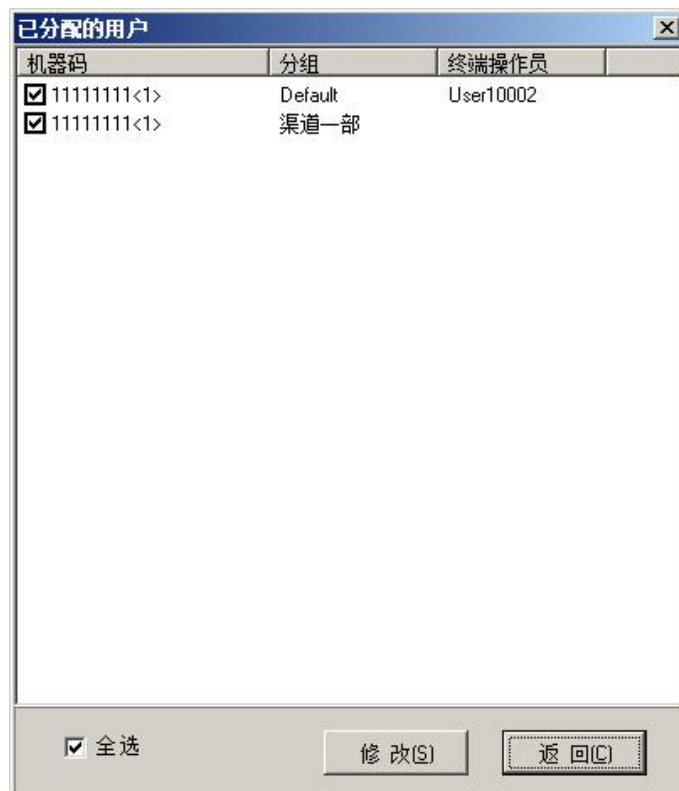
计算机机器码获取方法：把“获取机器码工具.exe”发给合作单位运行，把获取到的计算机机器码发给管理员添加即可。

管理员在控制台的功能栏选择“文件加密”-“外发设置中心”，弹出“外发设置中心”窗口中选择“机器码白名单”，在窗口右侧右键鼠标选择“添加机器码”，在“机器码”窗口中输入客户名称、相应的机器码及备注，点击“保存”。添加好的机器码就可以分配给相应的用户使用。如下图所示。



已增加的机器码可以修改、删除或清空机器码，可以查看某一机器码已经分配给哪些用户。

右键选中要查看的机器码，选择“已分配的用户”，弹出已分配情况窗口，可以根据需要修改分配设置。如下图所示：

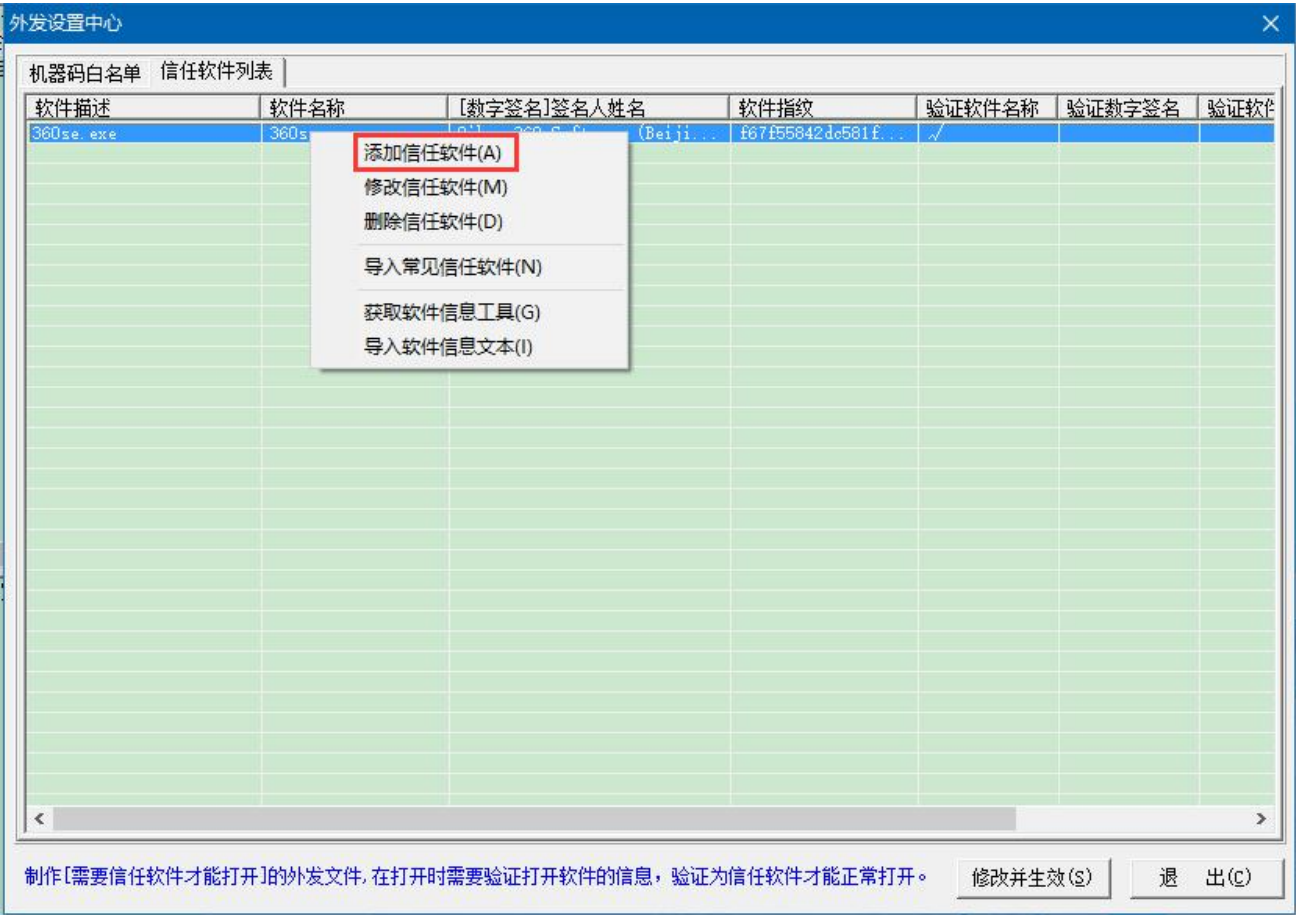


2.13.2 信任软件列表

可以将经常使用到的软件添加到“信任软件列表”里，终端用户在制作直接外发文件的时候，就可以把指定的软件添加到外发文件中，在打开外发文件的时候必须使用授权的信用软件才能打开文件。

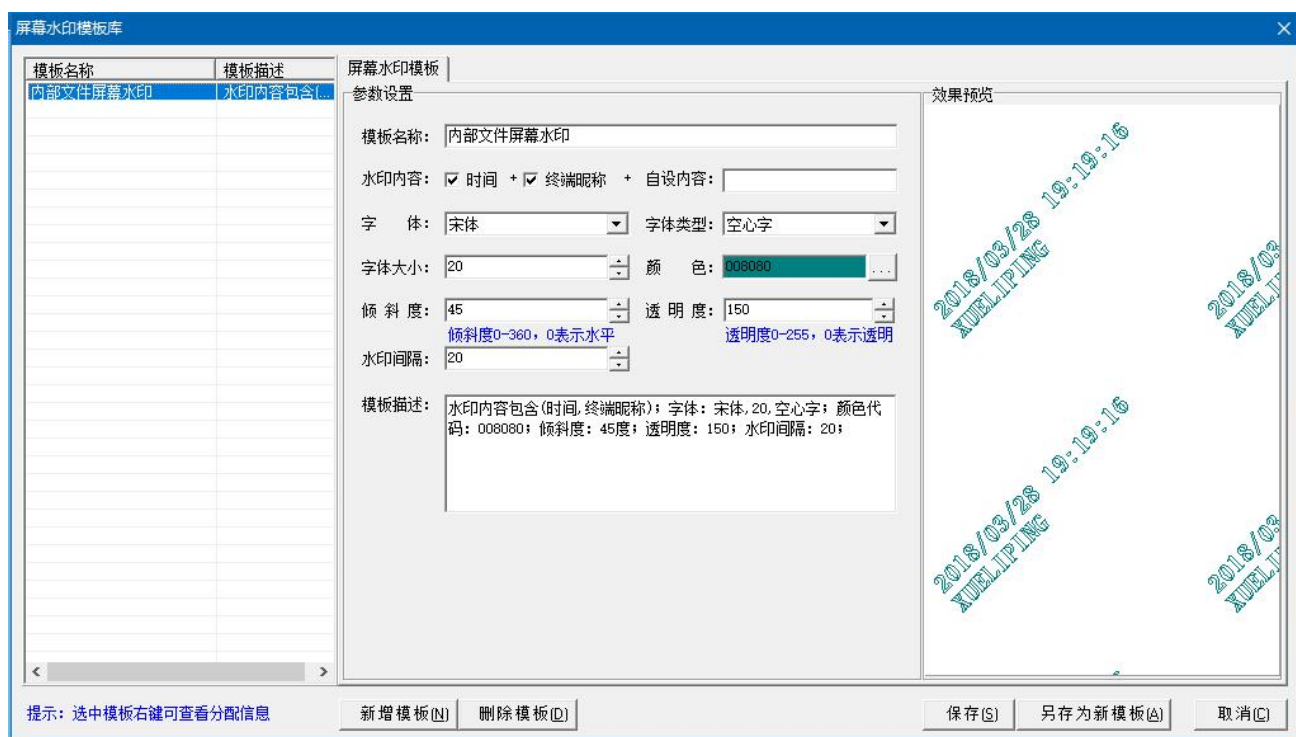
计算机信任软件信息获取方法：把“获取软件信息工具.exe”发到终端电脑上运行，把获取到的信息发给管理员添加即可。

管理员在控制台的功能栏选择“文件加密”-“外发设置中心”，弹出“外发设置中心”窗口中选择“信任软件列表”，并在窗口右侧右键鼠标选择“添加信任软件”，在“添加信任软件”窗口中的“软件描述”、“软件名称”、“签名人姓名”、“软件指纹”等地址栏内分别输入相应的数据，输入完成后点击“保存”即可。如下图所示。



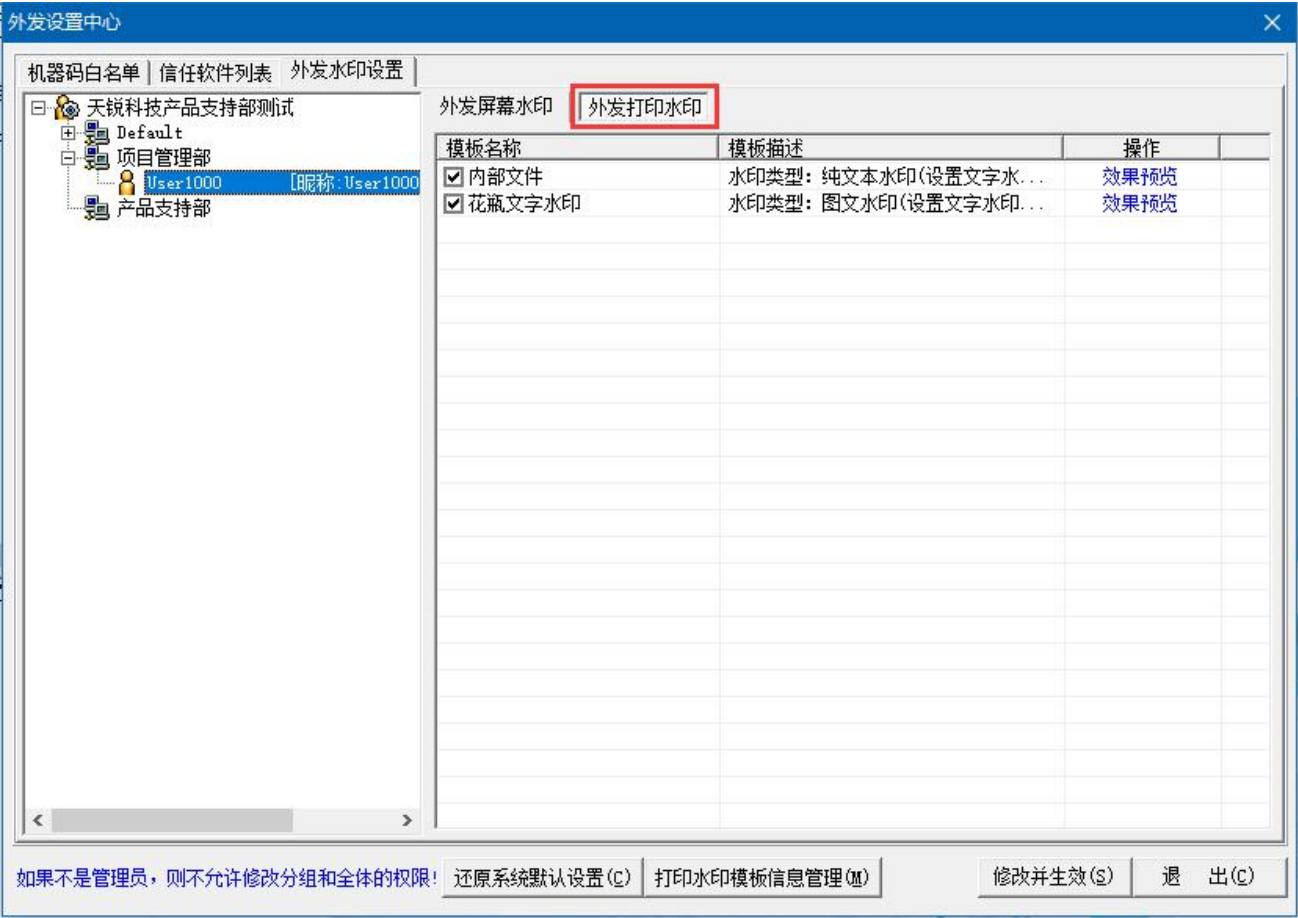
也可以选择“导入常见信任软件”，在弹出“导入常见信任软件”窗口中选择要导入的软件后，点击“确定”即可。如下图所示：



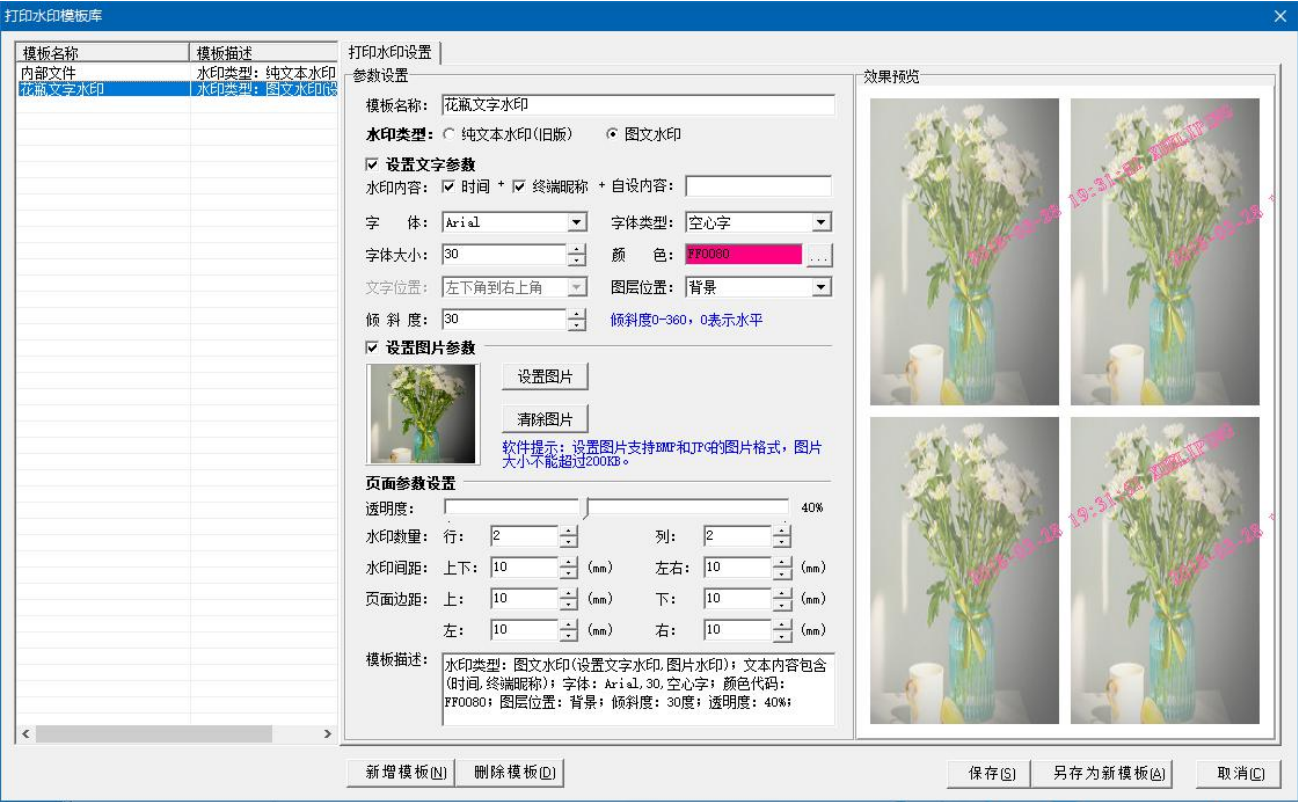


外发打印水印

管理员在控制台的功能栏选择“文件加密”-“外发设置中心”，弹出“外发设置中心”窗口中选择“外发水印设置”，在窗口左侧可以选择需要配置的对象，在窗口右侧打印水印列表中选择水印，可以点击后面的“效果预览”查看水印效果，设置完成后，点击“修改并生效”。如下图所示。



也可以通过“打印水印模板信息管理”设置外发打印水印，进行增删改水印信息。如下图所示：

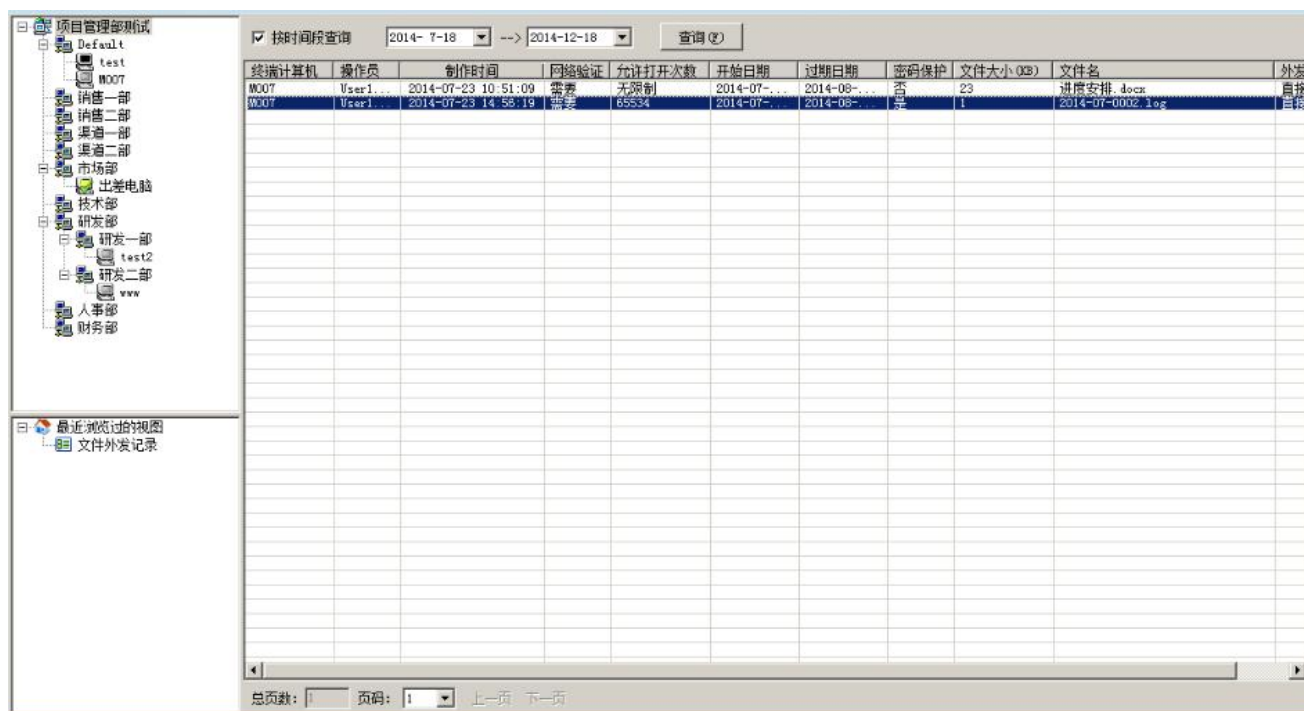


2.14 文件外发记录

2.14.1 查看文件外发记录

文件外发记录可查看有制作打印外发文件和制作直接外发文件权限的操作员的文件外发记录，通过流程申请的打印外发文件记录从“审批日志”中查看。

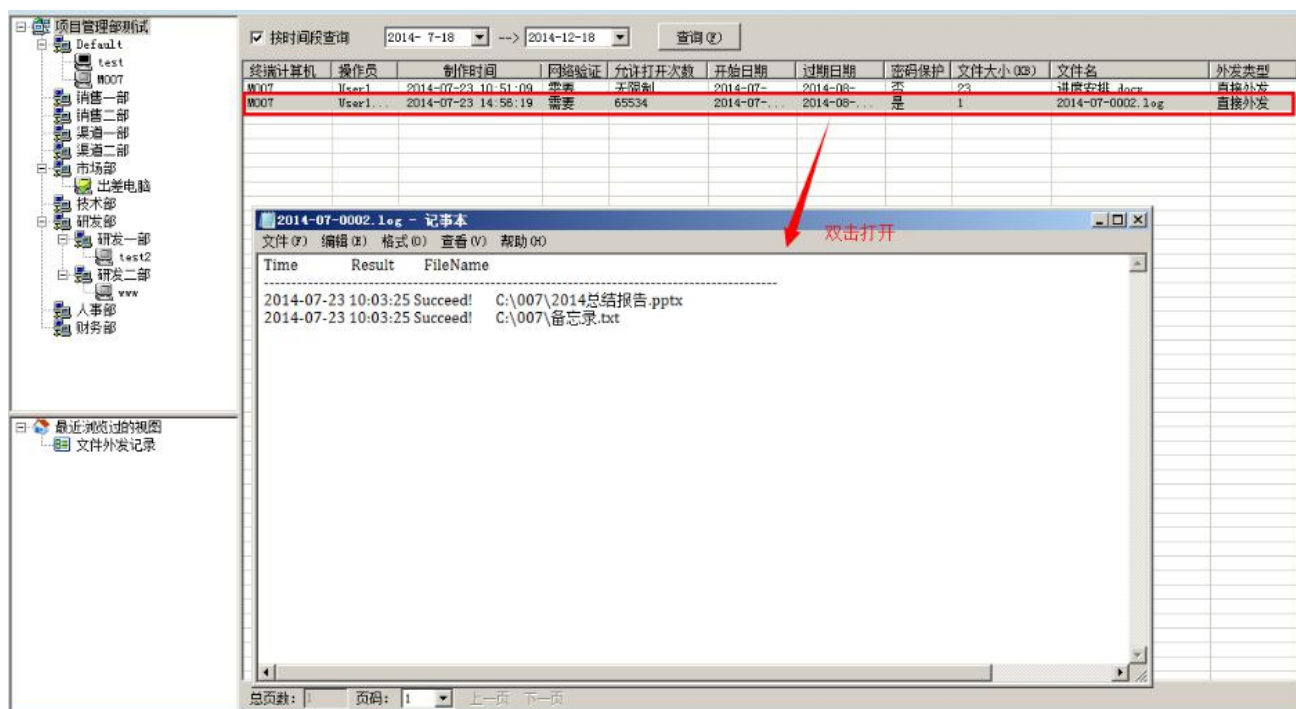
在控制台的功能栏选择“文件加密”-“文件外发记录”，用户列表栏选择要查看的对象（可以选择本地网络、分组或终端），在详细信息栏将显示选中用户当天的文件外发情况。文件外发记录信息包括：终端计算机、操作员、制作时间、是否网络验证、允许打开次数、开始日期、过期日期、密码保护、文件大小、文件名、外发类型等。可选择按某一具体时间或时间段查询文件外发记录：选择要查询的日期（打勾“按时间段查询”则可以按时间段查询文件外发记录），点击“查询”按钮即可查询对应时间的文件外发记录。如下图所示：



2.14.2 查看外发文件内容

管理员可以根据需要查看外发文件的内容。

查询出指定终端的外发文件记录后，在外发文件记录列表中选中需要查看内容的外发文件，双击即可打开并查看该文件的内容。如下图所示：



说明：申请解密与申请打印外发记录从“审批日志”里查看，右键下载可查看文件内容。

2.15 邮件白名单设置

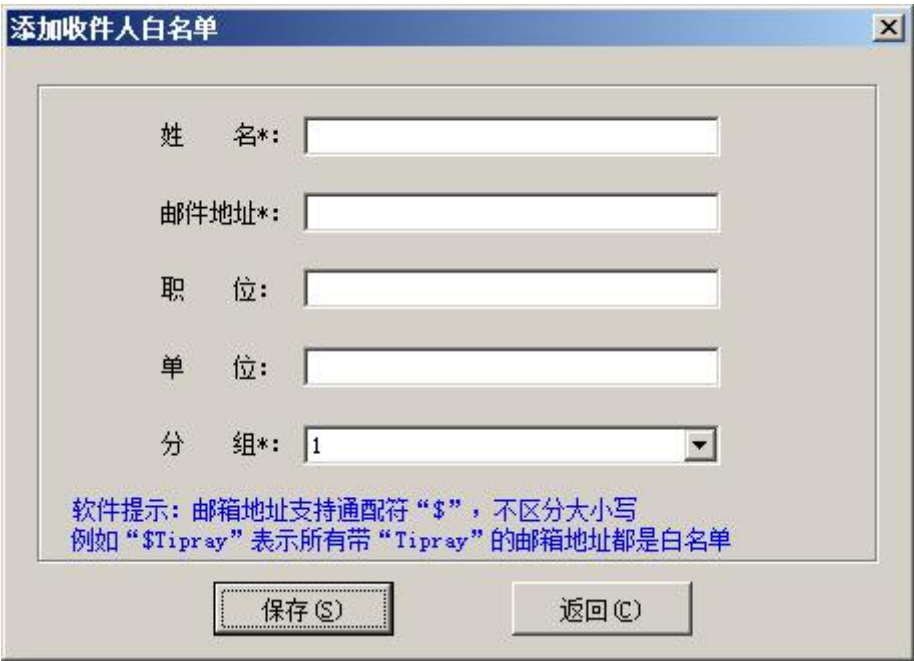
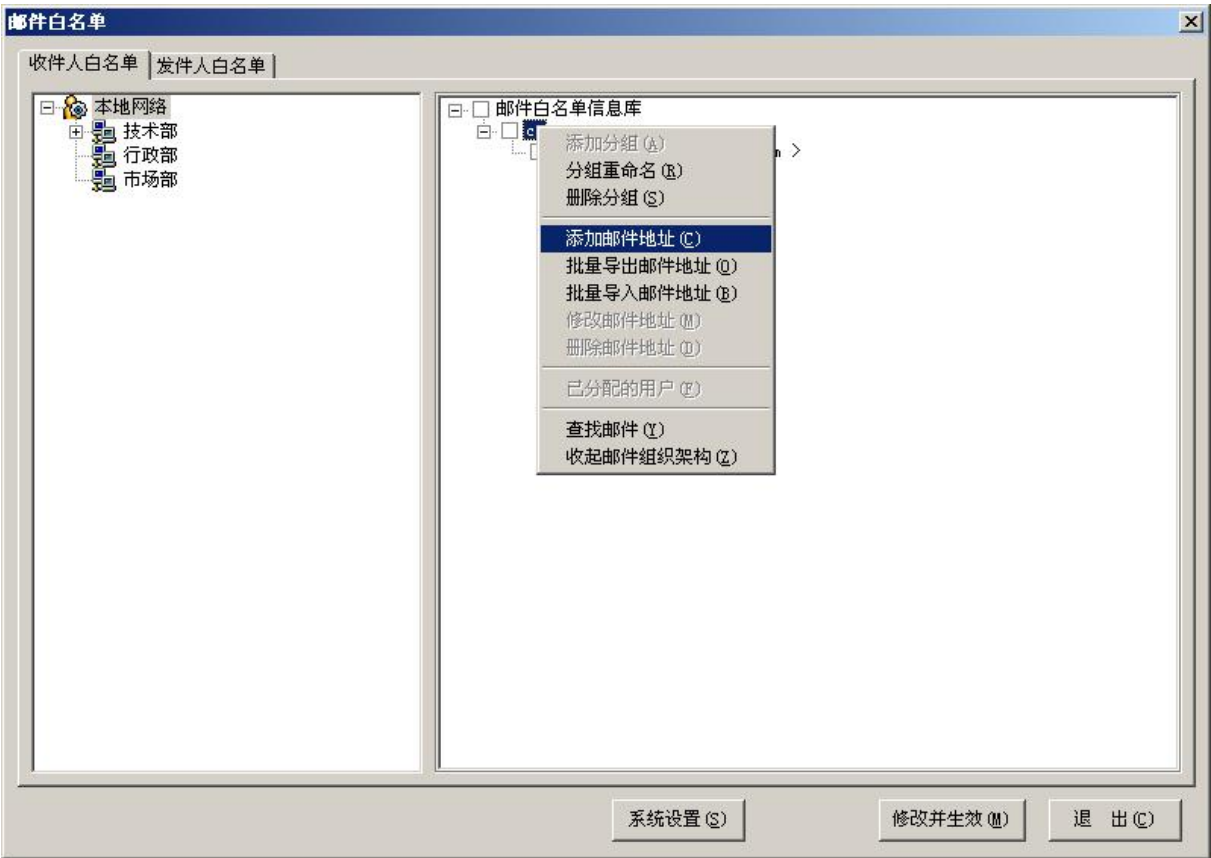
可以设置收、发邮件白名单，当终端用户使用天锐绿盾终端自带的邮件工具、outlook、foxmail 或闪电邮往白名单邮箱地址收、发送邮件时，加密的附件就会自动解密，减少解密申请次数，方便用户使用。

在功能栏选择“文件加密”-“邮件白名单设置”，弹出“邮件白名单”窗口，包含“收件人白名单”和“发件人白名单”两个子页面功能。

2.15.1 收件人白名单

添加邮件白名单

在“收件人白名单”页面，右键鼠标-“添加分组”，新建一个分组类别，然后选中新建的分组，右键鼠标-“添加邮件地址”，添加相应的邮件白名单信息库。邮件地址添加完毕，在窗口左侧的用户栏中选择需要设置邮件白名单的用户（可以选择本地网络、分组或终端），在窗口右侧勾选相应的邮件地址，然后点击“修改并生效”按钮即可。

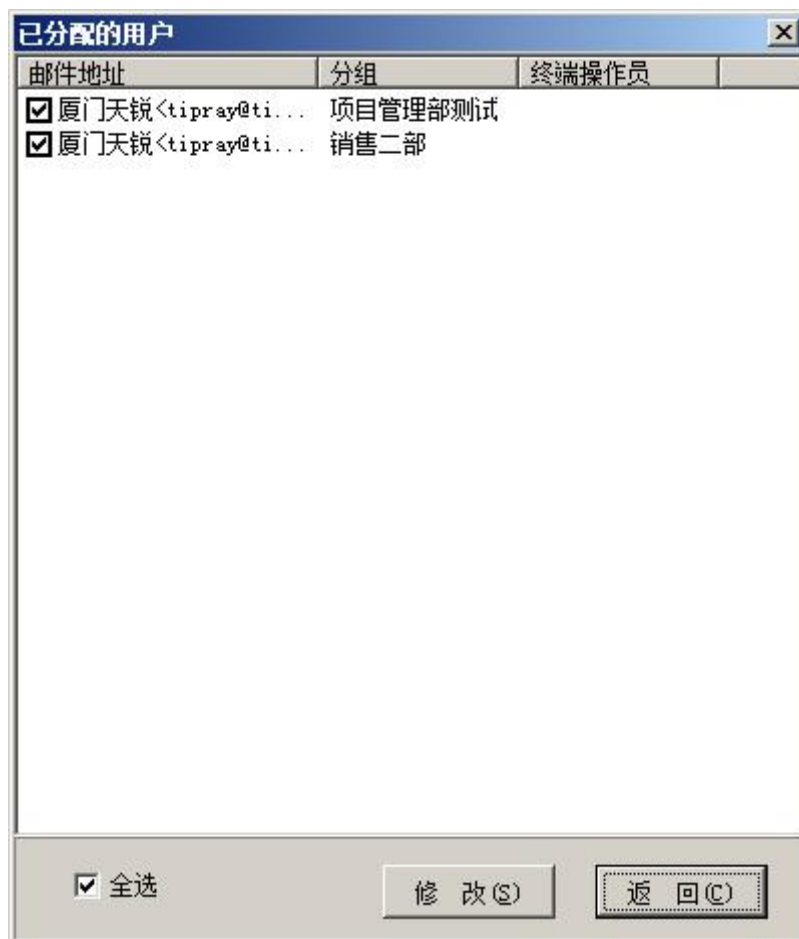


说明：邮箱地址支持通配符“\$”，不区分大小写，例如“\$Tipray”表示所有带“Tipray”的邮箱地址都是白名单。

添加好的邮件地址信息可以进行修改。右键选中需要修改的邮件地址-“修改邮件地址”，可以修改的邮件信息包括姓名、邮箱、职位、单位、分组。如果要删除邮件白名单地址，先去

除该邮件地址对所有终端的设置（若不去除将提示“邮件地址 xx 在使用中，不能删除！”），然后选中该邮件地址，右键鼠标-“删除邮件地址”即可。

要查看邮件地址已经分配给哪些终端用户，可以右键选中需要查看的邮件地址-“已分配的用户”，将列出该邮件地址已分配的用户所属分组及终端操作员名称，并可以直接修改分配信息。如下图所示：

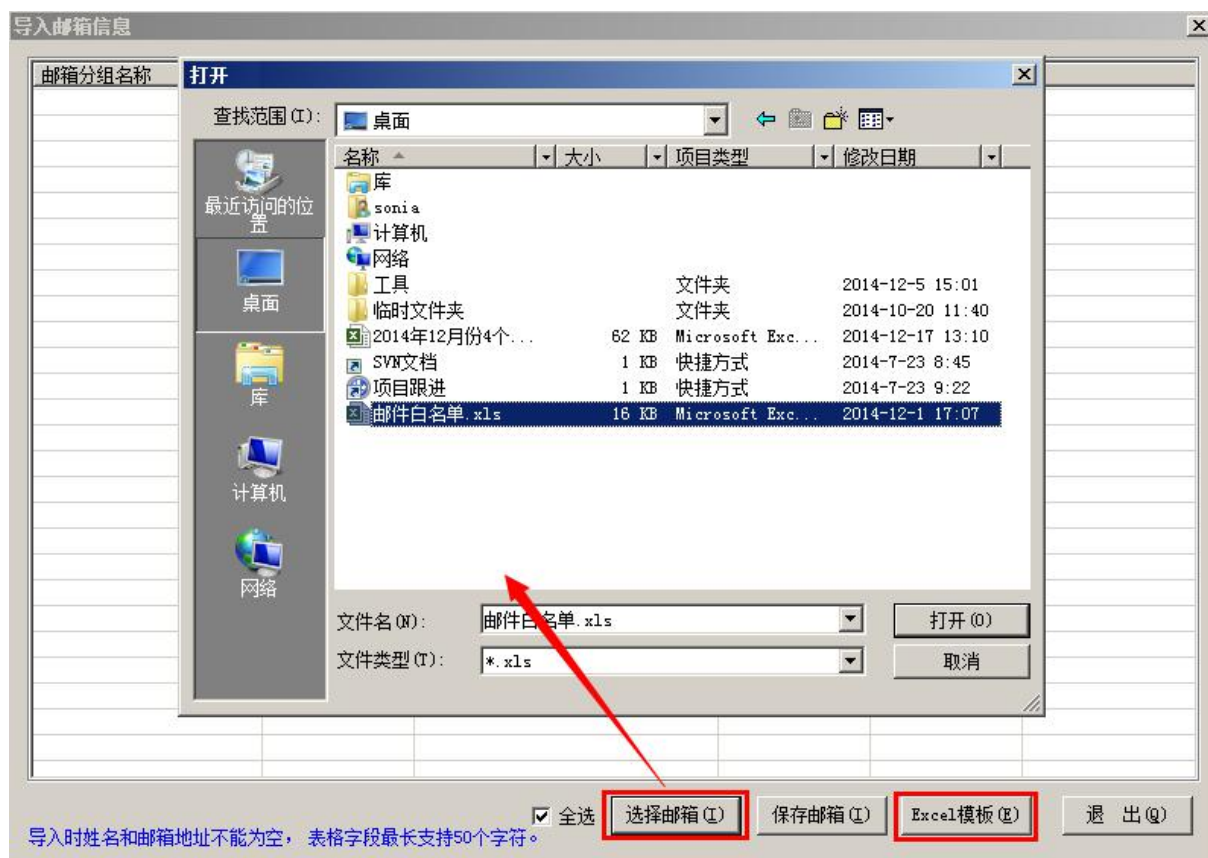


批量导入邮箱地址

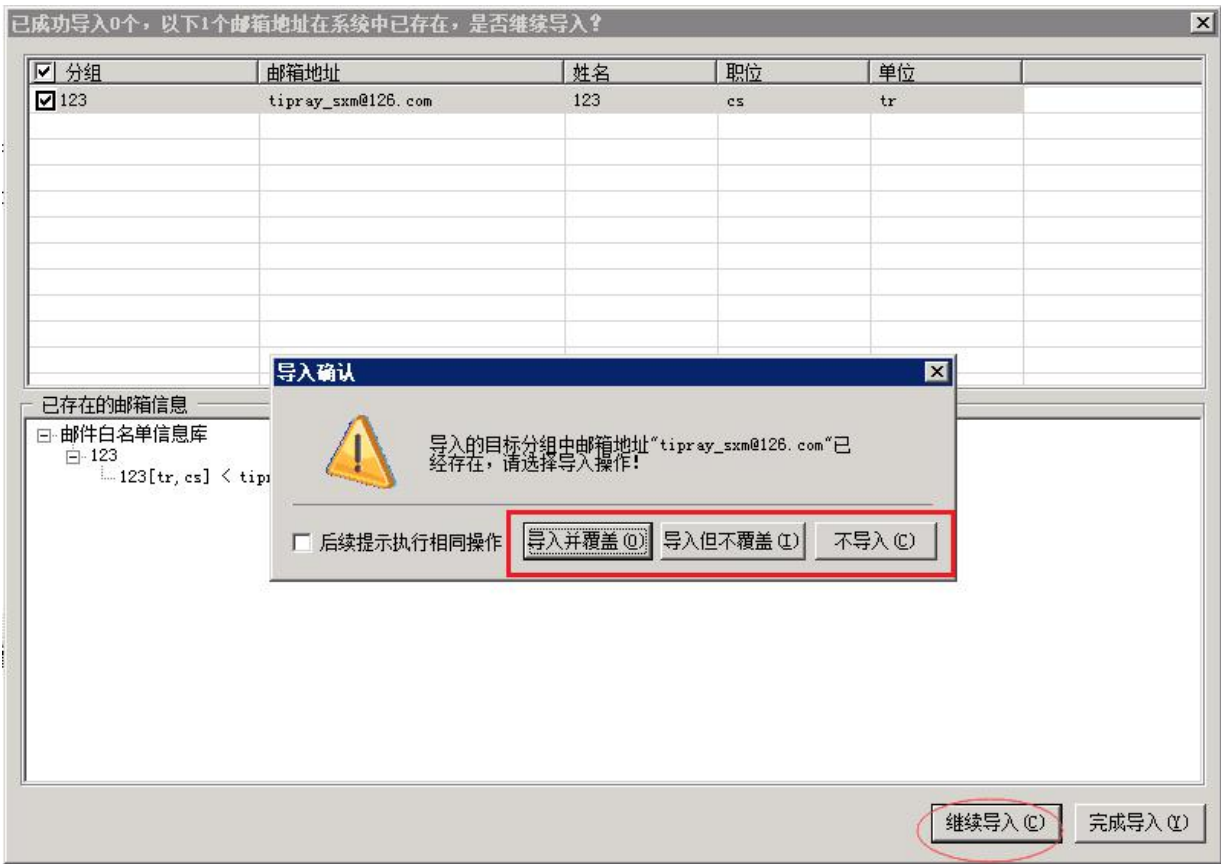
上述介绍的添加邮件白名单地址方式需要一个个添加，如果需要添加的白名单地址较多的情况下工作量就比较大，此时可以采用导入已有邮箱地址的方式来批量添加。采用导入邮箱的方式，需要先按要求制作好邮箱信息文档，包括邮箱分组名称、姓名、邮箱地址、职位、单位。系统也提供了 Excel 模块，可以参照模板进行整理。邮件白名单按部门进行分类，可能存在不同部门需要相同邮箱，现支持导入重复的邮箱地址，并且导入重复邮箱时会给予提示。

在“邮件白名单”窗口右侧，鼠标右键菜单选择“批量导入邮件地址”，弹出“导入邮箱信息”窗口，点击“选择邮箱”按钮打开要导入的邮箱地址文件。导入完成后，点击“保存邮

箱”，系统会根据 Excel 文档中的邮箱信息自动创建分组和邮件白名单。如下图所示：



如果导入的邮件白名单中，出现重复邮箱时，则跳出导入确认的弹窗提示。如下图所示：



批量导出邮箱地址

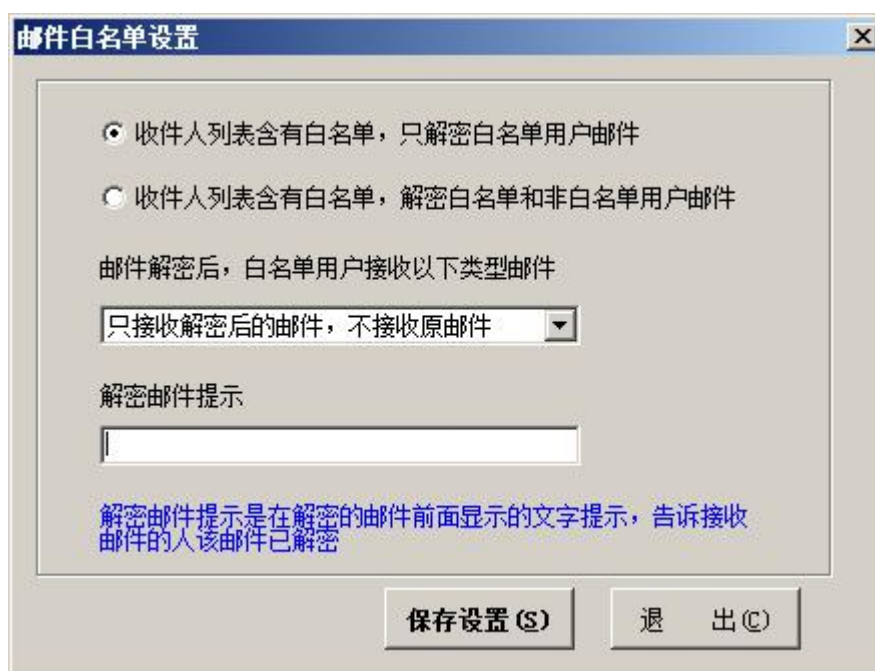
如果需要修改较多白名单地址的情况下，一个个修改的工作量会比较大，此时可以采用批量导出邮件地址方式，将所有的邮箱地址导出后重新修改整理，然后通过导入功能导入表格，从而达到邮箱地址的批量更新。

在“邮件白名单”窗口右侧，鼠标右键菜单选择“批量导出邮件地址”，弹出“另存为”窗口，选择要保存的地址后即可完成导出。如下图所示：



系统设置

设置邮件白名单的收件配置，可以根据实际使用需求设置。如下图所示：



“收件人列表含有白名单，只解密白名单用户邮件”：发件时，收件人中包含白名单地址

时，只解密白名单用户邮件，非白名单用户邮件保持原有的加密状态。

“收件人列表含有白名单，解密白名单和非白名单用户邮件”：发件时，收件人中包含白名单地址时，白名单用户邮件和非白名单用户邮件都解密。

“邮件解密后，白名单用户接收以下类型邮件”：设置白名单用户接收解密后邮件的类型，包括以下两种：

“只接收解密后的邮件，不接收原邮件”：白名单用户只接收解密后的邮件，不接收原加密邮件；

“接收解密后的邮件和原邮件两封邮件”：白名单用户接收两份邮件，解密后的邮件和原邮件。

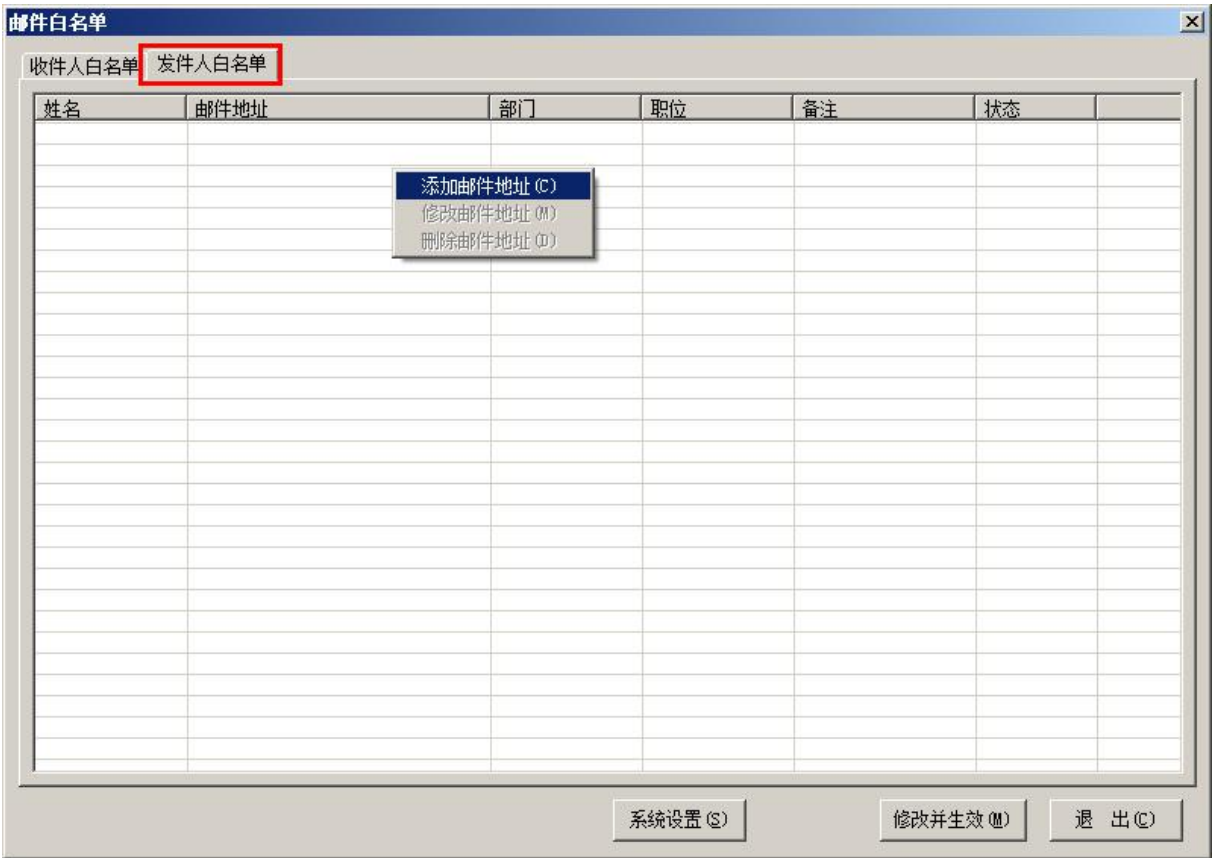
设置完毕后，点击“保存设置”即可。设置对所有用户生效。

注意：此处设置只对非 SSL 协议生效。

2.15.2 发件人白名单

使用发件人白名单邮箱地址发送邮件时，加密的邮件附件会自动解密。切换到“发件人白名单”页面，右键鼠标-添加邮件地址，弹出“添加发件人白名单”窗口，如下图所示。添加的发件人白名单可以通过更改状态来启用或禁用。

说明：Exchange 和 SSL 协议发送邮件，发件人不属于发件人白名单情况下，只要有一个接收人不属于接收人白名单列表内，则所有的接收人收到附件不会被解密。



2.16 服务器白名单设置

服务器白名单可以不改变企业网络架构，不用在应用服务器上安装任何软件的情况下，做到当加密文件上传到 OA 等应用服务器上时自动解密，下载到天锐绿盾终端电脑上时自动加密，保证数据在公司内上传、下载安全。

在控制台的功能栏选择“文件加密”-“服务器白名单设置”，弹出“服务器白名单”窗口，右键鼠标-“添加服务器地址”，新建一个新的服务器白名单。如下图所示：

添加服务器白名单

服务器描述:

地址类型:

服务器IP:

服务器端口:

上传行为:

上传文件类型: ☒ 所有类型

下载行为:

下载文件类型: ☒ 所有类型

浏览器进程名:

限制上传网速: B/s (字节每秒)
(-1表示不限制)

☐ 该规则生效 ☐ 是否验证服务器
☐ 使用代理模式白名单 (不推荐)

软件提示: 多个上传/下载类型之间以“|”分割。例如: . doc|. jpg
多个浏览器进程名之间以“|”分割。例如 iexplore. exe|Chrome. exe
验证服务器需要结合应用安全接入系统才可实现

“服务器描述”：添加的服务器白名单名称，可自定义。

“地址类型”：可以选择 IP 地址或域名，即服务器白名单的 IP 地址或域名。

“服务器 IP”：白名单服务器的地址范围

“服务器端口”：有效的白名单服务器端口。

“上传/下载行为”：可以根据实际情况设置为“解密”或“加密”，如果设置为“无”则不操作。

“上传/下载文件类型”：填写指定的文件后缀，可以勾选“所有类型”（即为*.*），这样只有指定类型的文件上传（下载）到服务器（终端电脑）才会自动解密或加密。

“浏览器进程名”：如果以上操作针对指定的程序生效，则点击“选择”勾选生效的进程。

“限制上传网速”：

“该规则生效”：该服务器白名单规则是否生效，默认规则是生效的。如果规则不生效，该条规则的状态将显示为“不生效”，此时即使把该规则分配给用户也不生效。

“是否验证服务器”：可以根据实际情况需要选择是否验证服务器，默认是不验证。

“使用代理模式白名单”：

服务器地址添加完毕，在窗口左侧的用户栏中选择需要设置该服务器白名单的用户（可以选择本地网络、分组或终端），在窗口右侧勾选上相应的服务器地址，点击“修改并生效”按钮即可。

2.17 审批流程管理

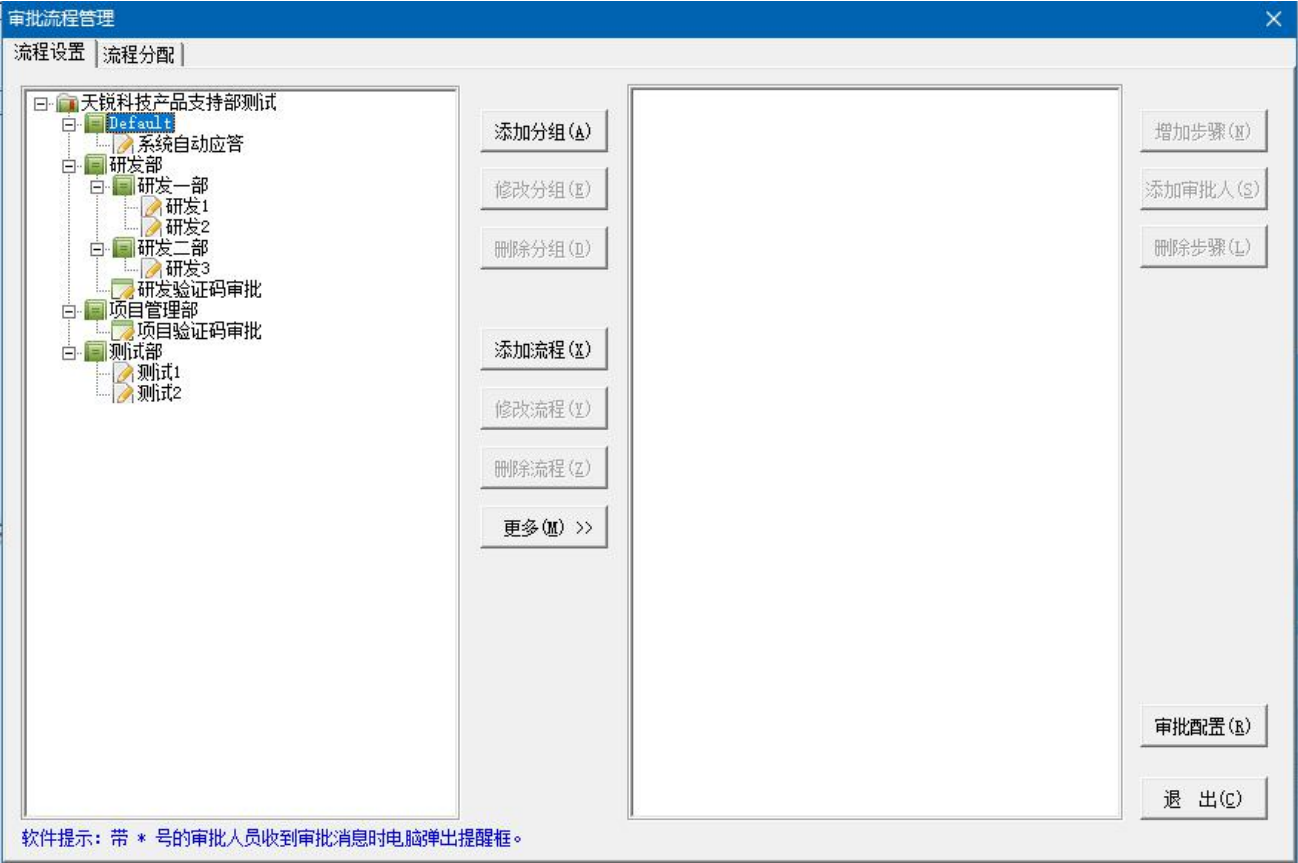
终端解密申请、离线申请、打印外发申请、直接外发申请和定密申请需要通过既定的流程进行，由指定的人员审批处理。可以对审批流程进行分组分类、支持增删改分组和流程、批量删除流程，并且支持导入导出审批流程。审批流程有普通流程和验证码流程两种方式。普通审批要求联网情况下才能够申请以及审批，而终端跟服务器无法通讯的情况下可以使用验证码审批方式进行申请以及审批。

用户可结合企业业务需要，自定义单级、多级审批流程（验证码审批目前支持单级审批流程），以满足不同的应用需要，同时，可以针对不同的分组、终端以及不同的申请功能设置多个流程，由多个操作员审批，使审批过程更灵活、更实用。

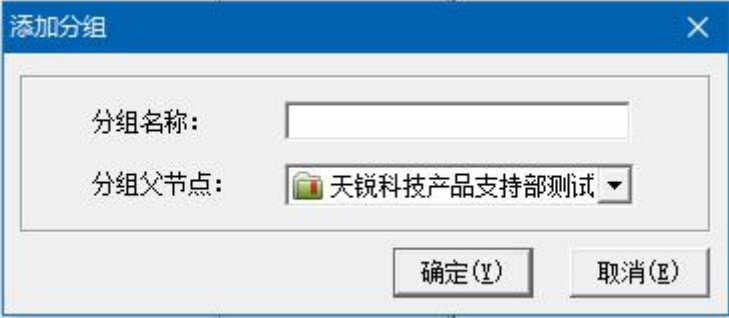
审批流程分为审批流程设置和分配两个操作步骤。审批日志可以查询当天或一段时间内审批的详细信息。

2.17.1 审批流程设置

在控制台的功能栏选择“文件加密”-“审批流程管理”，在弹出的“审批管理流程”窗口中选择“流程设置”页面，进行相关操作。如下图所示：

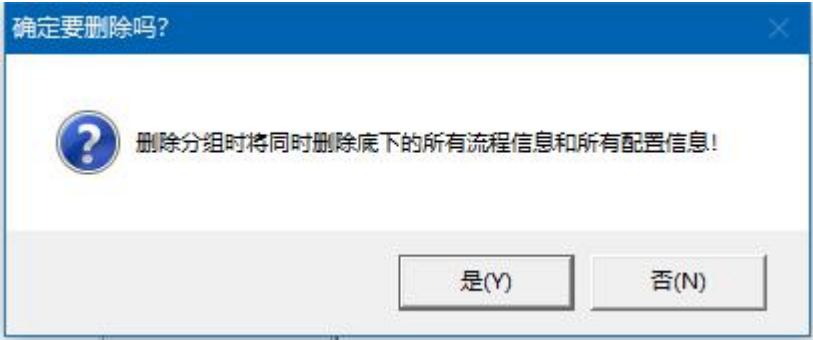


添加分组：单击“添加分组”按钮，输入要添加的分组名称，选择分组父节点。如下图所示：



修改分组：单击“修改分组”按钮，可以修改分组名称以及所属的分组父节点。

删除分组：单击“删除分组”按钮，弹出提示窗口，删除后将同时删除底下的所有流程信息和配置信息。如下图所示：



添加流程：单击“添加流程”按钮，选择要添加的流程类型，默认选择“普通流程”，然后输入流程名称和所属分组。流程名字可以自定义，可以添加多个流程。可设置高级设置，勾选“解密审批”则该流程只允许设置的对应密级申请该流程；勾选“解密、直接外发、定密审批”设置文件后缀，根据文件后缀名系统自动分配审批流程。如下图所示：



集成审批界面

添加审批流程

×

基本信息 | 高级设置

流程信息

功能类型：

☐ 解密审批

☐ 打印外发审批

☐ 离线审批

☐ 直接外发审批

☐ 定密审批

☐ 打印审批

☒ 阅读权限转换审批

所属流程分组：

【解密审批】

【打印外发审批】

【离线审批】

【直接外发审批】

【定密审批】

【打印审批】

【阅读权限转换审批】

流程类型：

☒ 普通流程

☐ 验证码流程

流程名称：

流程步骤

开始

➡

➡

结束

增加步骤(A)

设置审批人(Q)

删除步骤(D)

保存(S)

关闭(C)

添加审批流程

基本信息

高级设置

流程高级信息

☐ [解密审批]流程只允许申请如下密级的文件

☐ 公开文件☐ 内部资料文件☐ 秘密文件☐ 机密文件☐ 绝密文件

☐ [解密、直接外发、定密审批]流程申请文件后缀限制

每条申请记录必须包含如下后缀之一：

每条申请记录禁止包含如下所有后缀：

软件提示：文件后缀不区分大小写，全字匹配，后缀名前加“.”，多个后缀以“|”隔开。比如 .doc|.txt

☐ [解密、打印外发、直接外发、定密审批]流程智能自动审批

每个申请人在

当日

☐ 申请文件累计次数不超过 (次)
☐ 申请文件累计大小不超过 (MB)

软件提示：满足上述条件时，申请流程将自动审批通过，不需要流程审批人手动审批（累计只统计自动审批通过的申请文件次数和大小）。

☐ [解密、打印外发、直接外发、定密审批]流程申请限制

审批流程在

当日

☐ 申请文件累计个数超过 (个)
☐ 申请文件累计大小超过 (MB)

软件提示：满足上述条件时，申请流程将被限制，不能发起申请。

保存(S)

关闭(C)

独立审批界面

修改流程：添加好的流程可以修改名称和所属分组。如下图所示：

修改流程信息

常规设置

高级设置

流程类型：☒ 普通流程 ☐ 验证码流程

流程名称：

研发部

流程分组名称：

1

☐ [解密审批]流程只允许申请如下密级的文件

☐ 公开文件☐ 内部资料文件☐ 秘密文件
☐ 机密文件☐ 绝密文件

☐ [解密、直接外发、定密审批]流程申请文件后缀限制

申请文件必须包含如下后缀之一：

申请文件禁止包含如下所有后缀：

软件提示：文件后缀不区分大小写，全字匹配，后缀名前加“.”，多个后缀以“|”隔开。比如 .doc|.txt

确定(Y)

取消(N)

修改审批流程

基本信息

高级设置

流程信息

功能类型：

☐ 解密审批

☐ 打印外发审批

☐ 离线审批

☐ 直接外发审批

☐ 定密审批

☒ 打印审批

☐ 阅读权限转换审批

所属流程分组：

【打印审批】

流程类型：

☒ 普通流程

☐ 验证码流程

流程名称：

演示流程

流程步骤

开始

→

[指定操作员]:
User19877

→

结束

增加步骤(A)

设置审批人(Q)

删除步骤(D)

保存(S)

关闭(C)

删除流程：不需要的流程可以删除，删除流程前，先确认该流程没有在使用中。流程删除后，与该流程有关的所有配置信息也同时被删除。如下图所示：

确定要删除吗？

?

删除流程将同时删除有关的所有配置信息！

是(Y)

否(N)

另外还可以快速查找流程、查看流程已分配给了哪些用户、导入导出流程以及批量删除流程。如下图所示：



说明：系统自带了“系统自动应答”审批流程，该审批流程不能修改，也不能删除，可以重命名。属于该审批流程的用户，申请解密、打印外发等由系统自动应答，处理结果为通过。

添加好一个流程名称后，在“流程设置”窗口右侧会出现一个相应的流程图，在流程图开始和结束中间会有一个蓝色的节点（默认是 1 个，可以增加节点，最多不能超过 10 个节点）。如下图所示：



左键单击蓝色节点，或单击“审批人员分配”按钮，弹出“选择用户”窗口，在窗口左侧选择审批该流程的终端操作员。用户选择完毕，在窗口右侧将自动增加所选择的终端操作员，应答类型默认为“手动审批”，可以修改为其他类型。选择完毕单击确定即可，系统提示“流程保存成功！”，如下图所示。

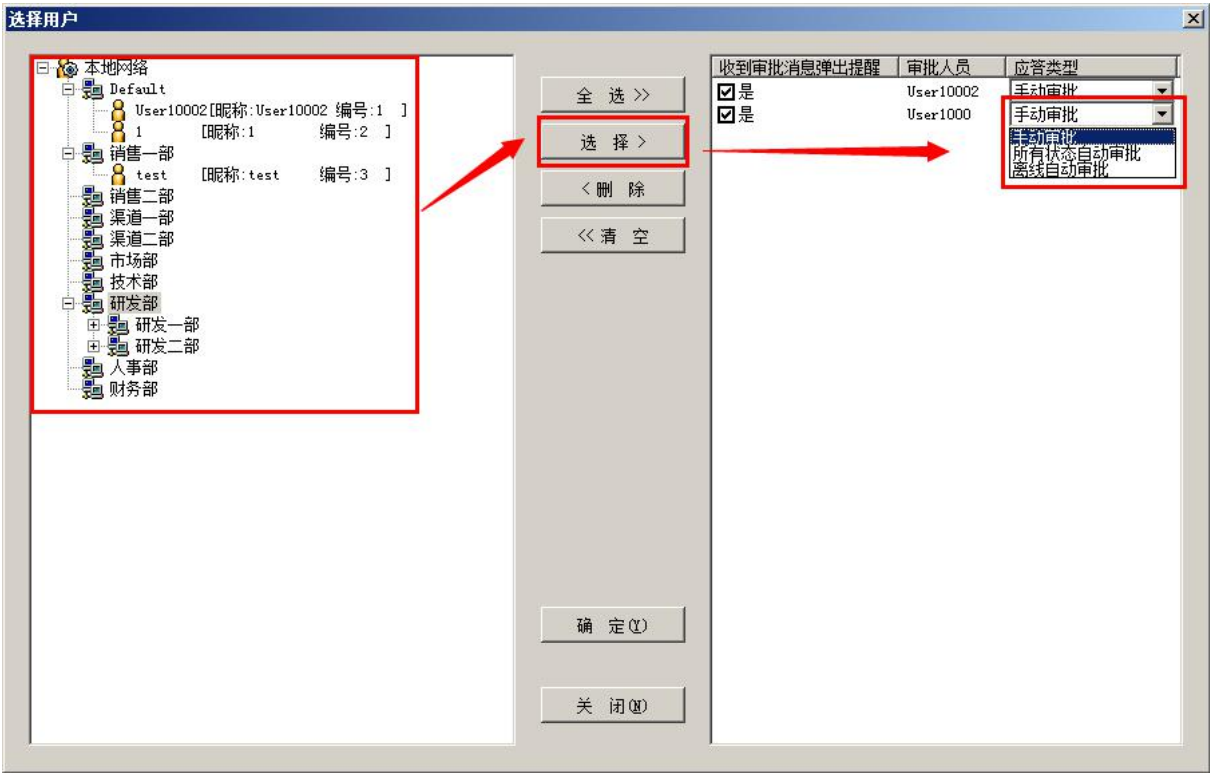
应答类型说明：

- **手动审批：**需要审批人员亲自受理，如果审批人员不在线或离开，审批将滞留；
- **所有状态自动审批：**不管审批人员是否在线，审批自动同意；
- **离线自动审批：**当审批人员不在线（不包括离开状态）的情况下，审批自动同意。

说明：

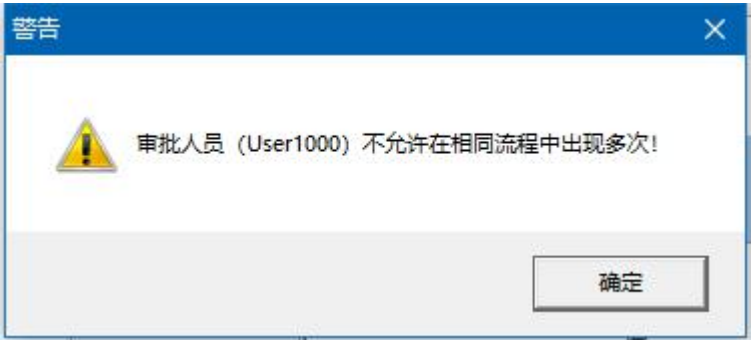
1、验证码审批流程应答类型只支持“手动审批”。

2、在“选择用户”窗口右侧，有个“收到审批消息时弹出提醒”的选择框，默认为“是”，这样审批人员收到审批消息时会弹出提示框。如果不想提示，可以去掉，即为“否”，这样审批人员需要通过点击右键“加密菜单”-“审批处理”或终端图标菜单列表中的“审批”-“审批处理”来查看申请消息。建议设置为“收到审批消息时弹出提醒”。



一个节点里可以拥有多个审批人员，通过在“选择用户”里同时选择多个操作员来实现。如果一个节点中有多个审批人员，申请者发出的申请请求几个审批人员都会收到，审批结果以服务器收到的第一个审批回复为准。例如：同一流程节点里有 User10022 和 User10023 这两个审批人员，他们会同时收到审批请求，如果 User10022 最早进行了审批处理，那么服务器就会保存 User10022 的审批结果，同意则让流程接着往下执行，不同意则返回审批结果，流程结束，同时 User10023 里的申请记录将自动删除。多个审批人员避免了如果审批人员不在，流程被迫停留在一个节点不能顺利执行。多人审批只要有一个操作员受理申请，流程就能顺利进行。

如果需要设置多级审批，单击“增加步骤”按钮，增加节点，添加用户的方式跟上面一致。在同一个流程中，出现在上个节点中的操作员，不能再出现在下面的节点中，否则会出现警告。
(验证码审批流程不支持多级审批) 如下图所示：



此外，可以对审批流程进行限制，包括终端一次申请的记录数、上传到服务器的单个文件大小等进行限制，超过限制值不上传到服务器，以减少服务器负荷。审批配置对所有的流程生效。如下图所示：



“单次最多可申请的记录数”：默认为 30 条，设置范围为 1~100 条，超过限定的条数，可以使用文件夹方式进行申请。

“上传单个文件最大值不能超过”：默认为 0，表示不对上传的文件大小进行限制，-1 表示不上传。

“离线申请的最长离线时间”：默认 180 天，设置范围为 1~720，超过最长离线时间则无法申请。

“上传文件后再发送申请”：对申请的文件上传到服务器的先后顺序进行限定，默认是先发送申请再把申请的文件上传到服务器，如果勾选了“上传文件后再发送申请”，则要等文件上传到服务器后才会发送申请，效率较慢。

“接收人信息和申请信息设为必填项”：勾选该设置后，终端用户在申请解密、打印外发、直接外发时，须填写接收单位、接收人姓名及申请原因后才能发送申请。

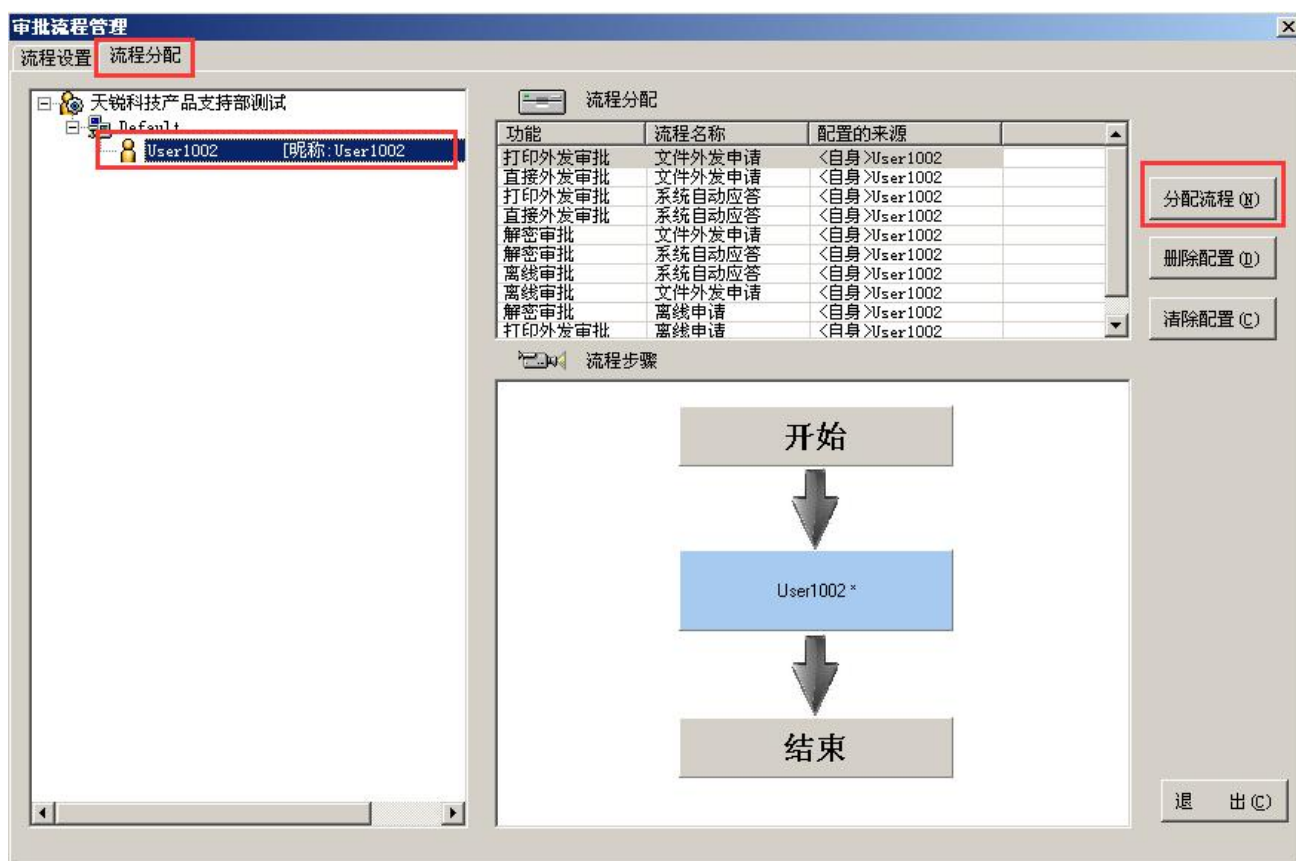
“不允许申请大小超过最大值的文件”：限制申请文件的大小，如果超过设置的最大值则申请失败。

“终端申请流程隐藏“验证码流程”类型”：终端申请审批可以隐藏已分配的验证码类型的流程。终端可以通过组合键 CTRL+ALT+鼠标左键调出。

2.17.2 审批流程分配

审批流程设置好了，就可以给终端操作员分配流程，设置分组或操作员执行哪些具体的流程和流程对应的操作，具体的操作如下：

1、在控制台的功能栏中选择“文件加密”-“审批流程管理”，在弹出“审批流程管理”窗口中选择“流程分配”页面，在窗口左侧选择要设置的对象（本地网络、分组或终端操作员），然后单击“分配流程”按钮。如下图所示：



2、在弹出的“分配流程”窗口中，对应各申请功能，分别勾选相应的审批流程。设置完毕，点击“保存配置”返回上级窗口。如下图所示：

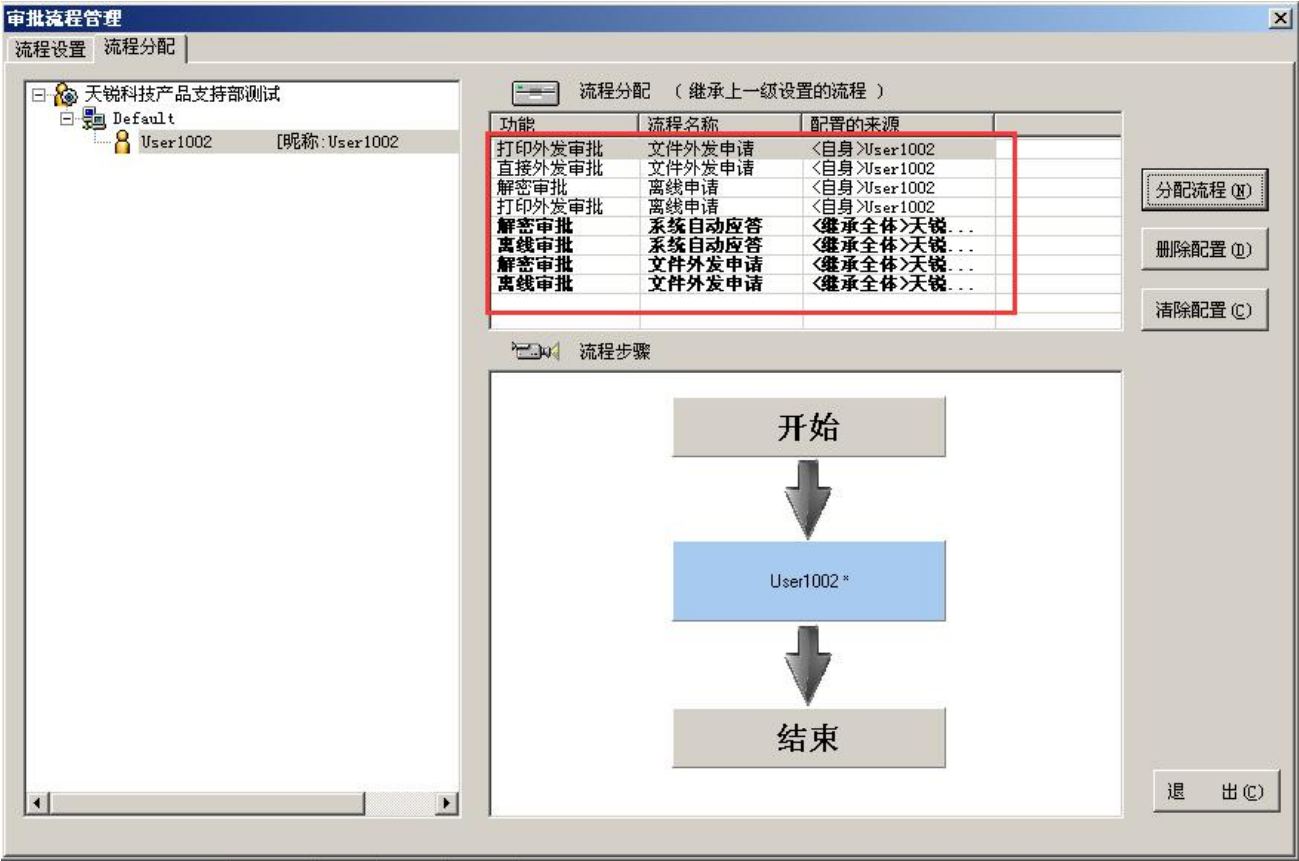


分配好的流程，如果要修改，可以点击“分配流程”按钮重新选择，如果要删除设置好的流程，先选中要删除的流程，再点击“删除流程”按钮。删除流程只能删除“配置的来源”属于“自身”的审批流程。

流程分配好之后，操作员做相应的操作就会按既定的流程来执行。

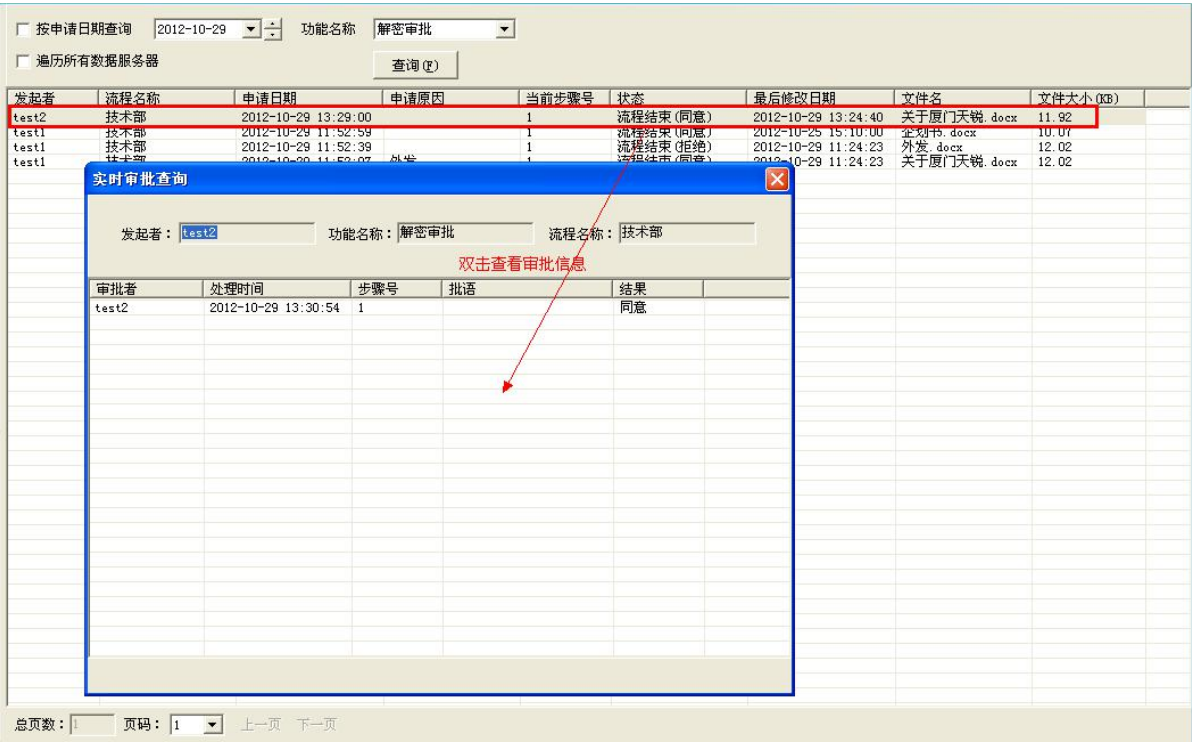
说明：如果在上述窗口中勾上了“所选 用户/分组 继承上一级设置的流程”（默认是勾选），那么所设置的用户或分组将继承上级设置的所有流程。

继承的审批流程的功能名称、流程名称、配置的来源以粗体显示，如下图所示。“配置的来源”信息中显示流程是属于自身的流程还是继承分组的流程。继承的审批流程不能删除，若点击继承的审批流程，“删除流程”按钮将失效，以灰色显示。

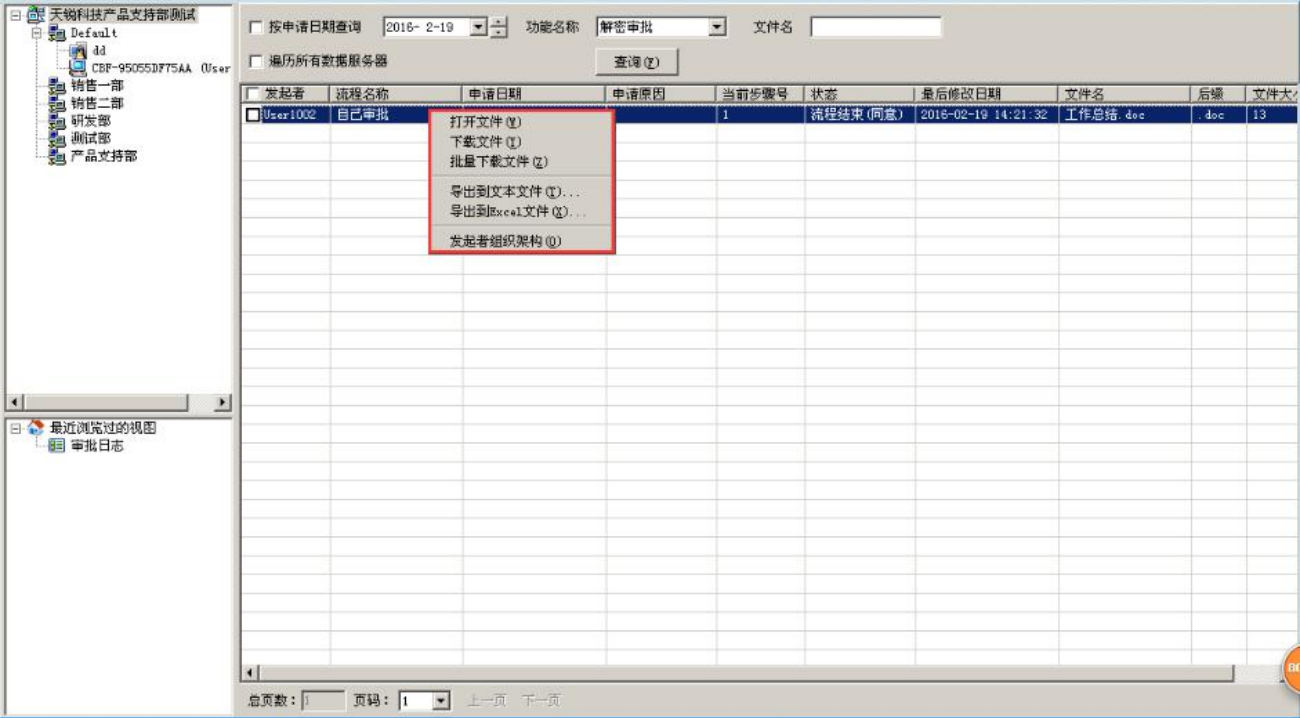


2.17.3 审批日志

终端通过审批流程申请解密、申请打印外发、申请离线、申请直接外发的情况可以从审批日志中查看，可以按本地网络、分组、终端、时间段、功能名称分开查询。记录信息包括申请者、流程名称、申请日期、申请原因、申请状态（结果）、申请的文件名、文件大小及文件内容。双击记录可查看审批详细信息：发起者（申请人），功能名称、流程名称、审批者、处理时间、步骤号、批语、结果。如下图所示：







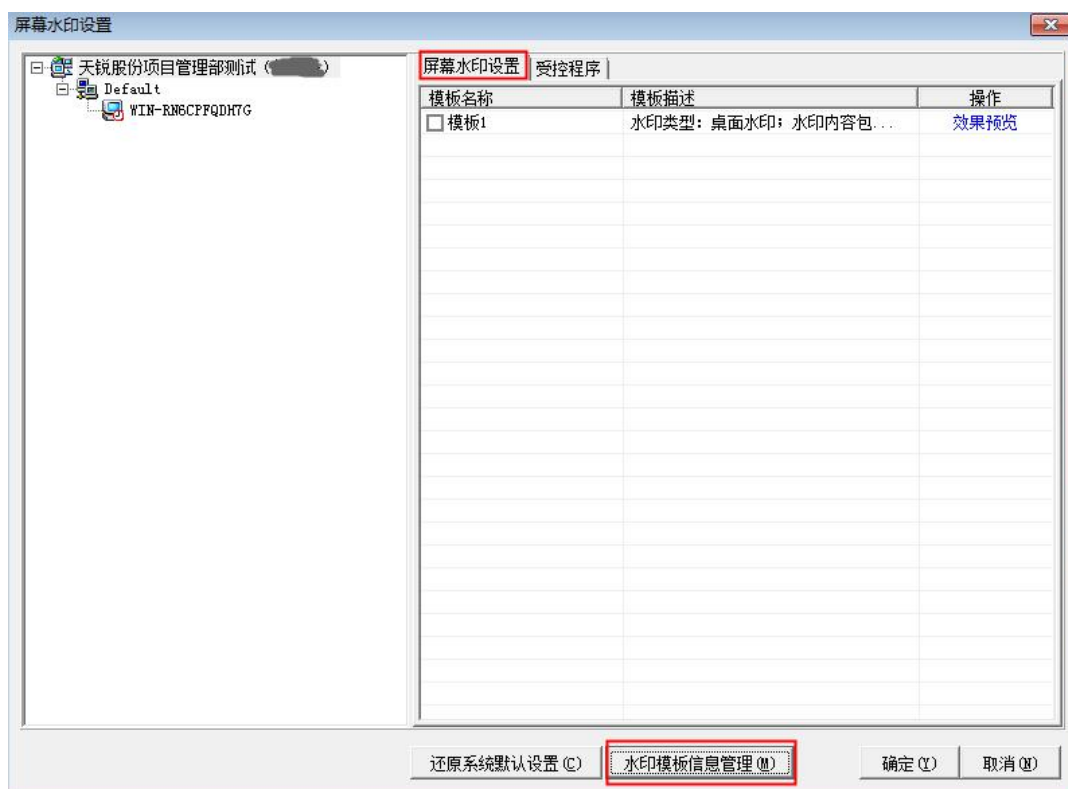
申请解密、申请打印外发、申请直接外发的文件内容在服务器上也可以查看，选中审批记录，右键选择打开文件或下载文件。也可把审批记录导出到文本文件或 Excel 文件进行存档，供日后查看。如下图所示：



2.18 屏幕水印设置

通过屏幕水印设置，可以对指定进程设置屏幕水印，有效保障了企事业单位资料的版权。

在控制台的功能栏中选择“文件加密”-“屏幕水印设置”，弹出“屏幕水印设置”窗口，用户信息栏中选择需要设置的终端或分组，在窗口右侧设置屏幕水印模板以及设置受控程序。点击“水印模板信息管理”弹出“屏幕水印模板库”窗口设置屏幕水印模板名称，选择水印类型。设置水印内容，水印内容包括时间、日期、IP 地址、MAC 地址、计算机名称、计算机登录用户名、操作员名称及自设内容等。还可以对水印内容的字体类型、大小、颜色、形式、位置、形式（包含文字水印、点阵水印）进行设置，选中“水印选项”点击按钮“”则选中的内容即为水印内容，点击按钮“”则为全选；若要删除则在“水印设置选项”中选中内容点击按钮“”即可，点击按钮“”则将设置的水印全部删除；同时可根据水印选项中的“空格”和“空行”对水印内容进行自定义布局并可以根据需要自定义图层前景或背景显示。如下图所示：如图所示：



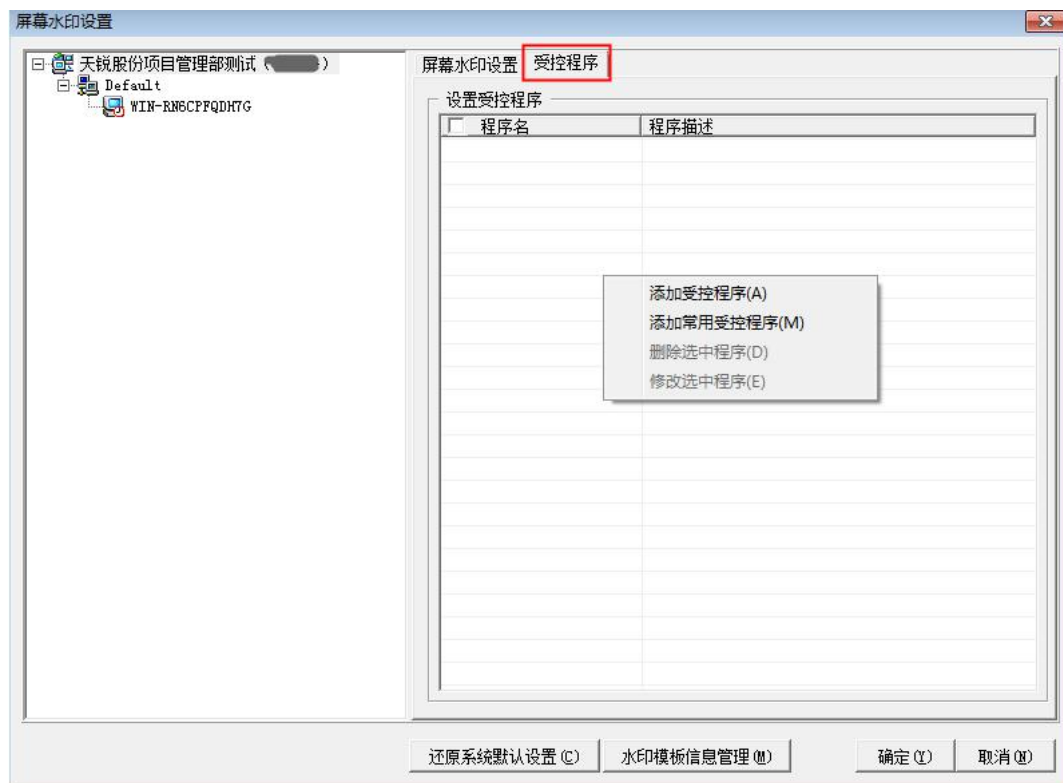


“文字水印”屏幕文字水印是在整个桌面或进程上显现计算机相应的信息，水印信息包括自定义信息和操作者信息（终端昵称、时间、IP 地址和 MAC 地址等），管理员直接查看视频或者照片*能知道是从哪台计算机上泄露出去的。

“点阵水印”屏幕点阵水印是将整个电脑屏幕或进程界面覆盖上一层包含自定义水印内容（包含时间、终端昵称、操作员名称、IP 地址、MAC 地址）的圆点图案。当机密信息被拍摄外传时，管理员在照片上获取点阵水印图案后，可以通过控制台的【查询点阵码】得到泄密信息来源的

相关信息（包括计算机名称、用户名称、IP、时间等），防止屏幕信息被泄露后出现无据可查的现象。

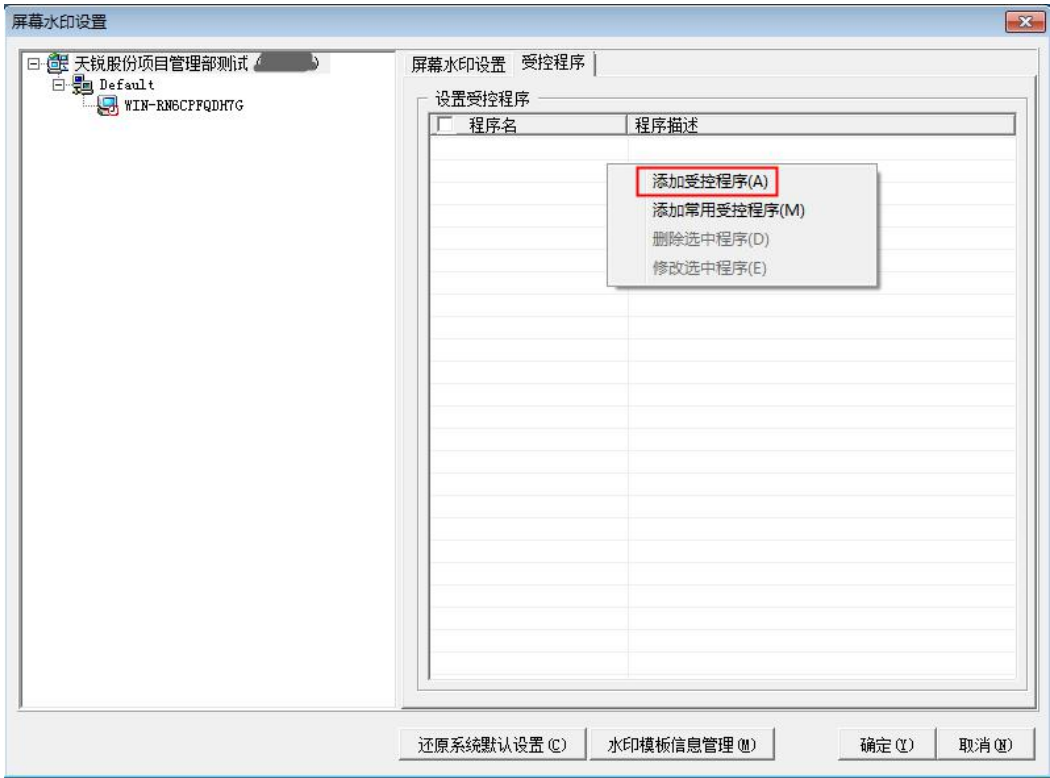
屏幕设置完成后，要添加受控程序，并给终端或分组配置，屏幕水印才能生效。在控制台的功能栏中选择“文件加密”-“受控程序”右键，系统会弹出提示，如下图所示：



选择“添加常用受控程序”，弹出“常用受控程序”窗口，勾选需要添加的受控程序后，点击“确定”即可。如下图所示：



也可以点击选择“添加受控进程”，弹出“添加受控进程”窗口，在相应的地址栏处填写正确的信息后，点击“确定”即可。如下图所示：





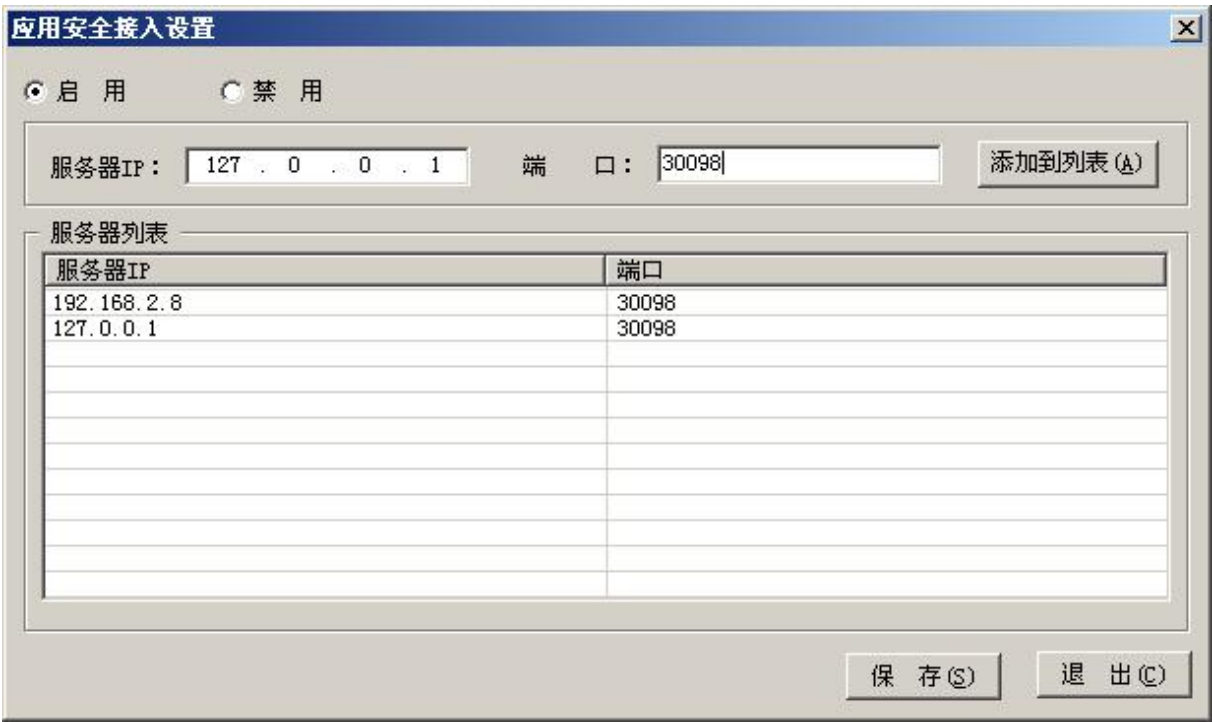
受控进程添加完成后进行分配，在用户信息栏选择要分配的终端或分组，右侧勾选要配置的受控进程，设置完成后，点击“确定”即可。

2.19 应用安全接入设置

通过服务器白名单功能，可以对终端电脑数据强制透明加密，对上传到应用服务器数据自动解密。服务器白名单只能管控到有安装加密客户端的电脑，安装加密客户端的终端用户只要拥有账号和密码就可以轻松访问应用服务器，这将会很容易导致重要数据的泄露。

为此，还需要对应用服务器的安全接入做进一步的管控。“应用安全接入设置”模块，主要是与天锐绿盾接入系统进行结合，从终端身份识别、传输隧道加密等多方面进行应用数据安全访问控制，确保访问受控应用系统的终端合法性以及数据传输过程的安全性。


在控制台的功能栏中选择“文件加密”-“应用安全接入设置”，弹出“应用安全接入设置”窗口，选择单选框“启用”或“禁用”后，在“服务器 IP”和“端口”地址栏处输入天锐绿盾接入系统的服务器 IP 地址和端口号，输入完成后，点击“添加到列表，该记录会成功添加到服务器列表中，点击“保存”按钮即可。如下图所示：

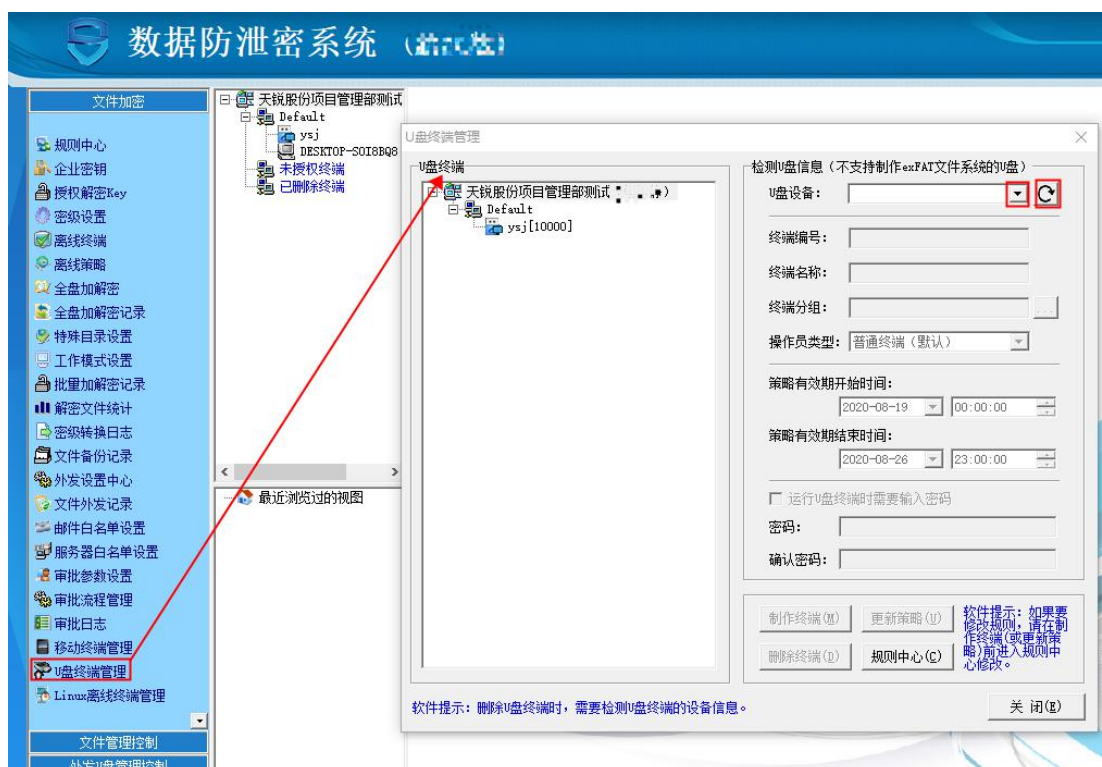


控制台模块配置完成后，同时要对天锐绿盾接入系统服务器进行设置，同步天锐绿盾数据库防泄密系统的终端用户，才可以正常使用，详细操作步骤参考《天锐绿盾应用服务器安全接入系统使用说明书》中 5. 与天锐绿盾结合使用。

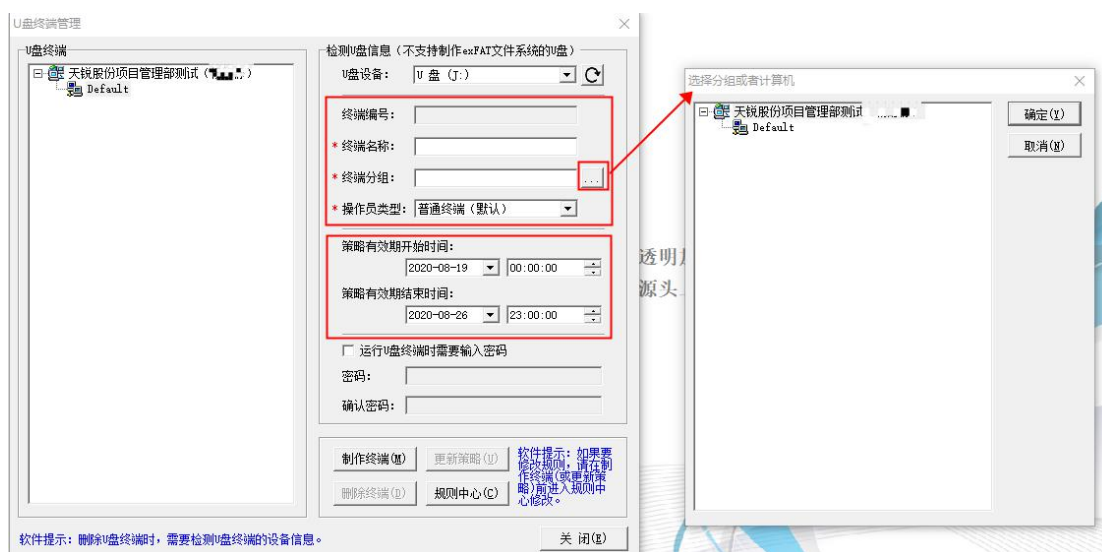
说明：天锐绿盾接入系统如何对应用服务器的安全接入进行管控，可参考《天锐绿盾应用服务器安全接入系统使用说明书》文档。

2.20 U 盘终端管理

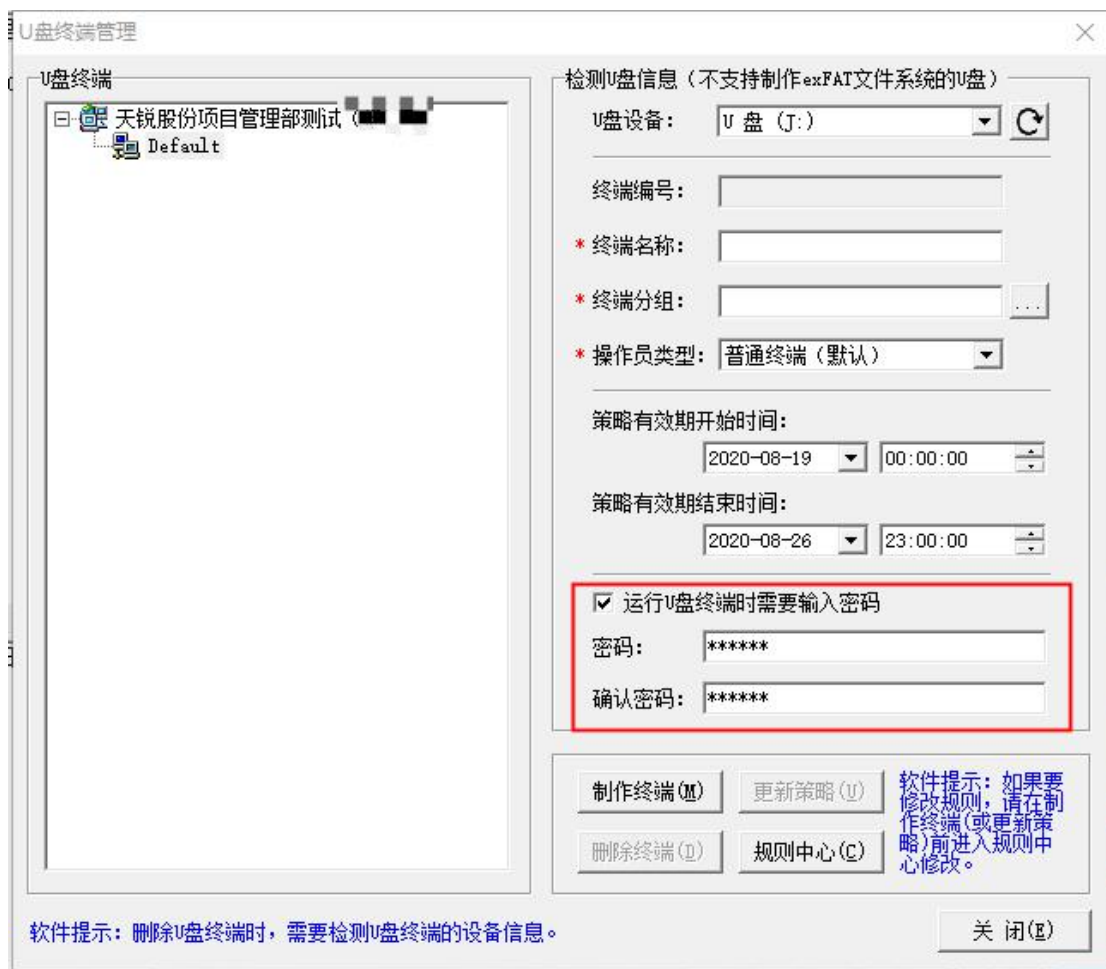
在“文件加密”中点击“U 盘终端管理”菜单弹出 U 盘终端管理界面，插入普通 U 盘，点击刷新按钮“”，系统检测出 U 盘设备，如果有多个 U 盘，点击下拉按钮即可选择要制作成 U 盘终端的 U 盘，如下图：



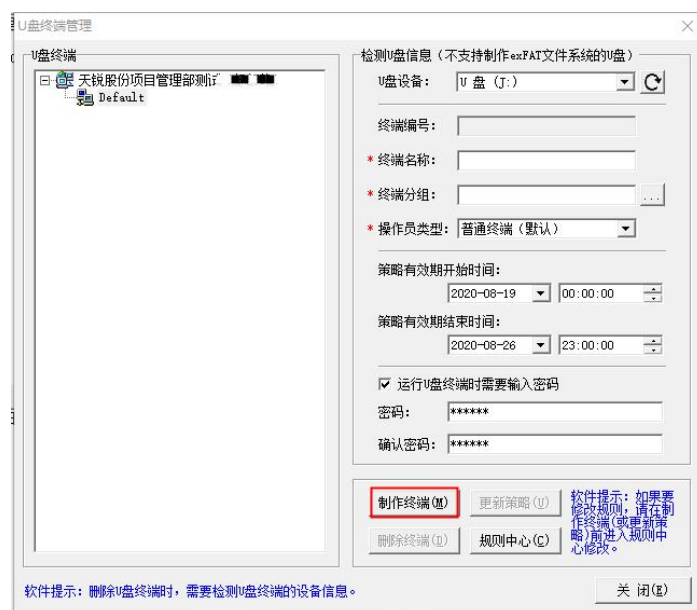
检测出 U 盘之后，设置该 U 盘终端的名称、分组和操作员类型，同时设置策略的有效时间如下图：

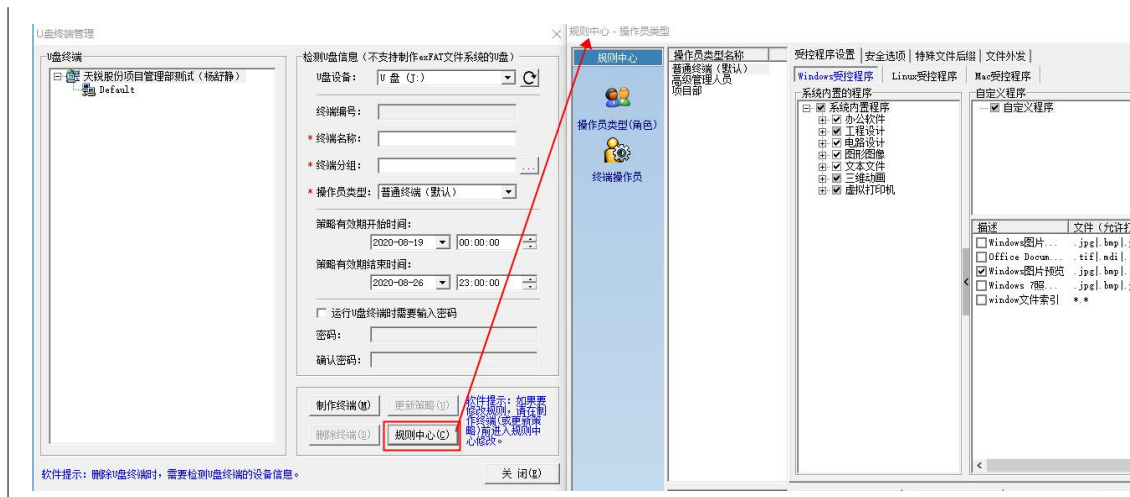


勾选“运行 U 盘终端时需要输入密码”，设置该 U 盘的运行密码，则终端用户使用该 U 盘时需要进行输入密码才可运行，如下图：



如果要修改策略则在更新策略和制作终端之前点击“规则中心”进入规则中心界面修改策略，修改后关闭规则中心界面，点击“制作终端”即可。已制作完需要更改策略，在规则中配置好后，点击“更新策略”即可。若需要删除终端，在检测到该终端时，点击“删除终端”即可。如下图：





2.21 外发 U 盘

企业常把一些重要的电子文档资料通过邮件、聊天工具等方式发送给客户或者合作伙伴，然而这些外发文档很容易被非法篡改、无序传播、甚至存在安全泄露等风险，使得企业所做的大量工作付之一炬，严重危害了企业的利益。

天锐绿盾外发 U 盘系统是软硬件一体的文件外发媒介，用来保护企业外发文件的安全性和保密性，防止文件的二次扩散。为了增强外发文件的管控能力，企业可通过天锐绿盾数据防泄密系统对外发 U 盘进行统一授权管控，加密文件导入到外发 U 盘内可以正常阅读，并且文件导出保持密文，非法人员即使获取到也无法打开，只有在绿盾受控环境下方可使用。[无外发 U 盘导出权限的绿盾终端用户](#)，则无法导出外发 U 盘内的文件。

在控制台的功能栏中选择“文件加密”-“外发 U 盘管理”，弹出“外发 U 盘管理”页面，如下图所示：

[illegible]

“设置 U 盘策略”：已经授权的 U 盘，可以在控制台上直接设置 U 盘策略。点击“设置 U 盘策略”，弹出 U 盘管理员验证密码窗口，输入正确的密码后，可自动运行外发 U 盘，弹出管理员操作页面，对 U 盘策略进行设置。如下图所示：

天锐绿盾外发U盘

Tipray U-DISK External System

系统管理

资源管理

管理员

配置信息

配置信息

系统设置

U盘控制规则

文件控制规则

机器码白名单

用户密码规则

用户参数设置

密码管理

修改密码

设置密码问题

U盘认证控制:

使用次数:

使用开始时间:

使用结束时间:

不限制

不限制

不限制

修改配置

U盘文件控制规则:

允许打印:

允许截取屏幕:

允许保存修改内容:

过期后格式化U盘:

用户选择打开方式:

显示U盘权限信息:

允许

不允许

不允许

是

是

是

修改配置

U盘内外文件交互:

允许用户导出U盘文件:

允许用户导入文件到U盘:

不允许

不允许

修改配置

“解除授权”：在设备列表上，点击设备上的“解除授权”，授权解除且，删除所有该外发 U 盘的授权配置。

“基本信息”：设置“U 盘名称”和“备注”信息。

“使用对象”：设置导出权限。可以选择“添加操作员”或者按“添加部门”设置哪些对象具有导出权限，也可以删除指定对象或清空列表。

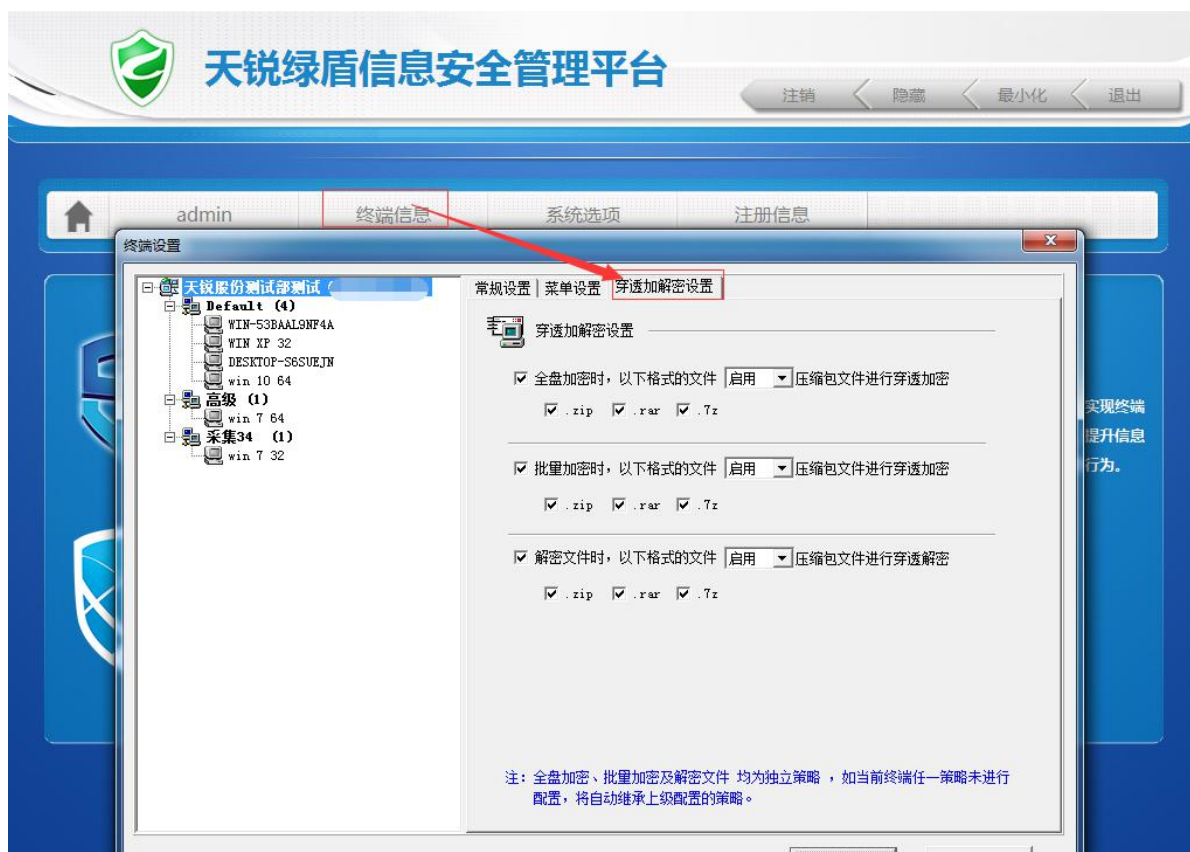
“保存/授权”：授权信息配置完成后，点击“保存/授权”，即完成 U 盘授权。如果当前 U 盘正在运行，则会提示先关闭后再保存。

说明：天锐绿盾外发 U 盘具体操作步骤，可参考《天锐绿盾外发 U 盘快速使用指南》和《天锐绿盾外发 u 盘使用手册》。

2.22 穿透加解密

穿透加解密是指对压缩包内的文件进行加解密，包括全盘加解密、解密审批、批量加解密三个操作。

终端需要开启穿透加解密权限需要由管理员到控制台进行配置，配置位置在：“控制台-终端信息-终端设置”。



菜单栏左侧选择对应终端，右侧勾选对应操作权限、支持压缩包格式以及是否启用，终端启用后后，操作对应功能时，窗口标题将有“已启用穿透加解密”提示,可以填写所需加密的文件后缀。



2.23 主辅 IP 切换

主辅 IP 切换是指终端可以设置两个服务器 IP（一般指同一个服务器的内、网 IP），终端

会自动识别当前与哪个服务器 IP 处于通讯状态，并提示用户是否切换到可通讯 IP。设置位置在：“点击终端图标—系统信息—系统设置—服务器配置”，输入需要配置的主辅服务器，选择是否立即生效（自动重启终端），点击保存即可。

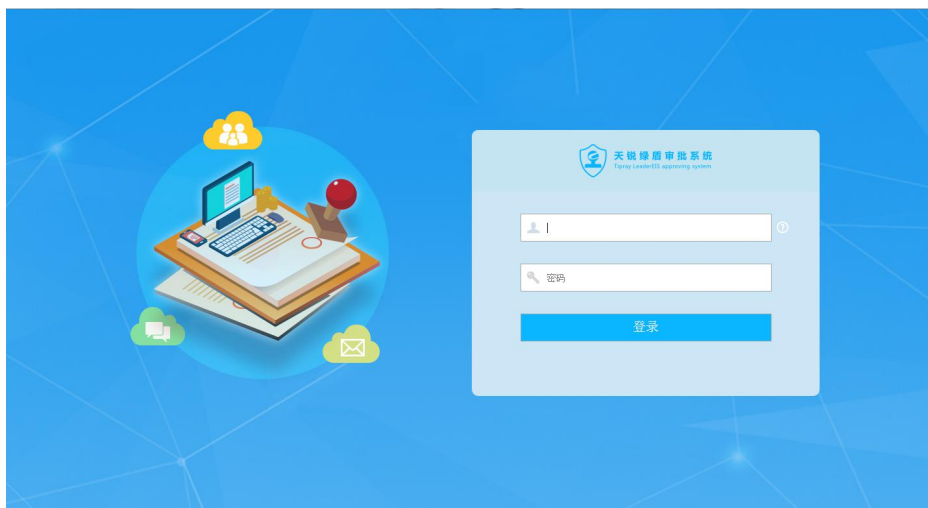


2.23 独立审批

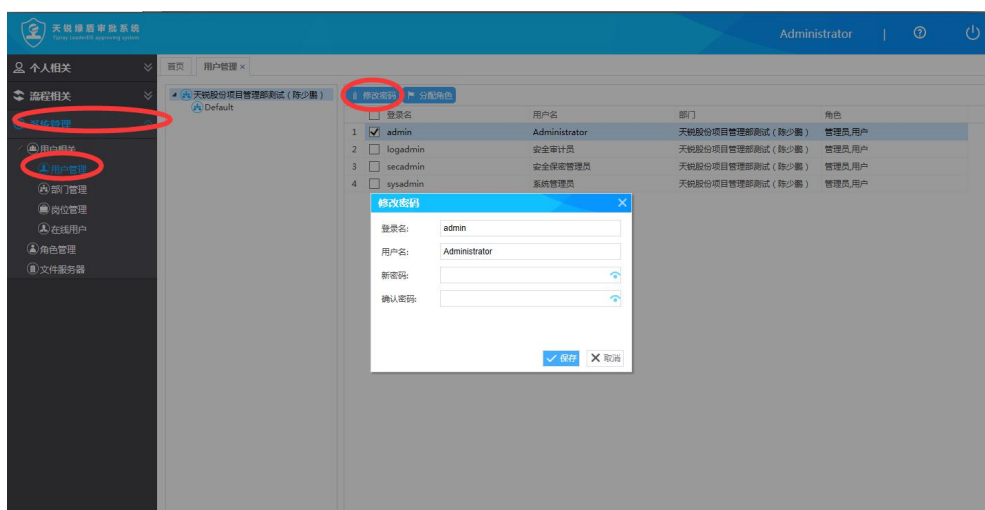
“安装独立审批服务器”：若要开启审批，安装完成绿盾服务器后，需安装独立审批服务器，选择一台服务器，目前支持 win7 server2008 及以上的 64 位的系统。打开独立审批服务器安装包，安装过程中需正确填写绿盾引擎服务器及其端口（默认端口为 20080），安装完成后，双机桌面审批服务器



，进入服务器登录页面，输入管理员账号：admin，密码：默认为空，点击登录。从地址栏可查看审批服务器端口，默认端口为：8180。

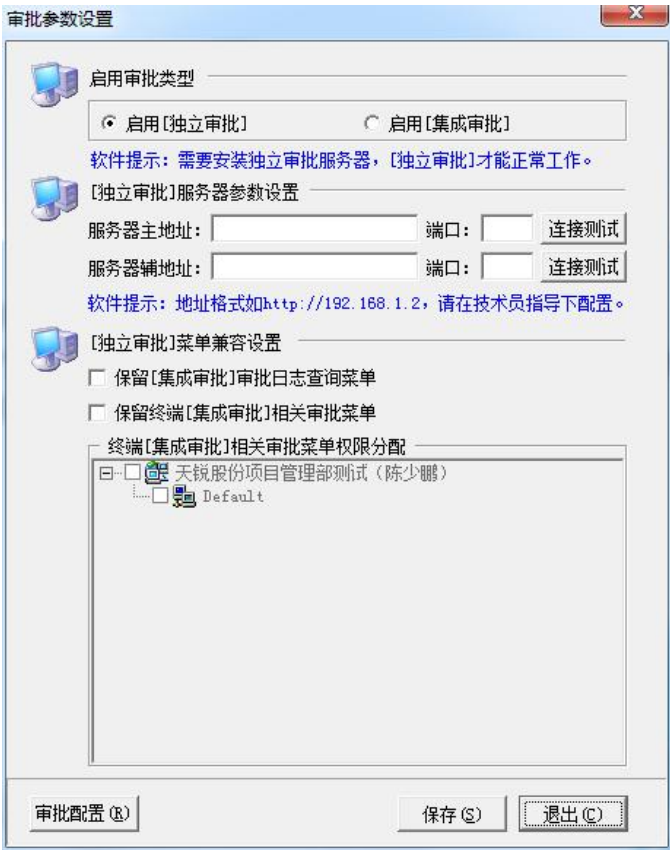


“修改管理员账号密码”：首次空密码登录后，系统自动提示修改密码，输入安全性较高的密码后，保存并熟记即可。若需要再次修改密码，需要进入**“系统管理”—“用户管理”**，勾选需要修改的管理员，点击修改密码即可。

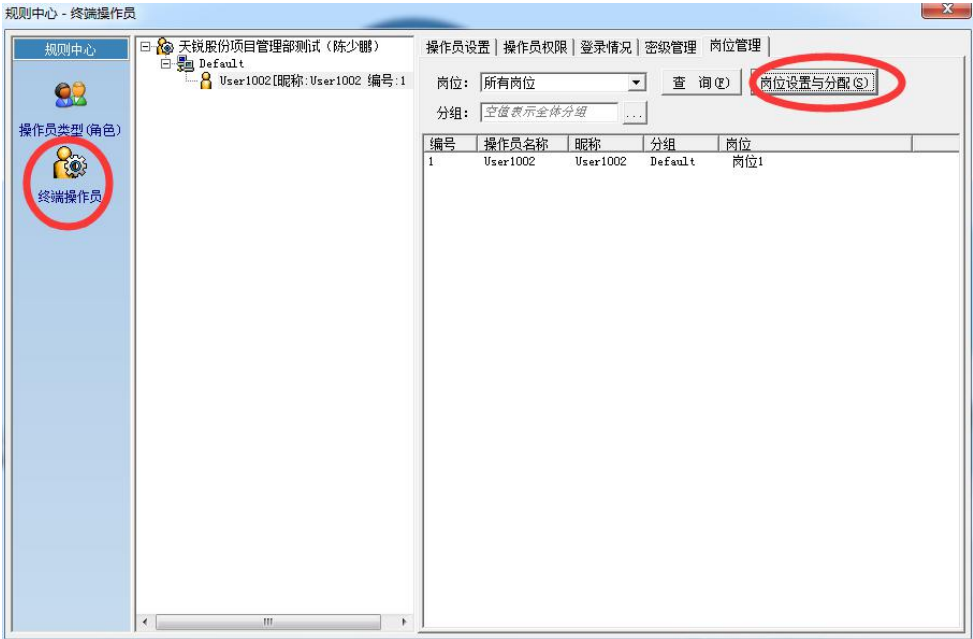


“查看是否与绿盾引擎连接成功”：修改密码后，可参看**“用户管理”**和**“部门管理”**是否将绿盾组织架构及用户同步成功，同步成功后，就可以到绿盾控制配置相关参数及流程。

“绿盾控制台设置参数”：完成独立审批服务器安装并成功连接到绿盾引擎后，打开绿盾控制台，依次点击天锐绿盾防泄密系统—**“审批参数设置”**，按界面提示配置相关参数。其中独立审批服务器地址为安装独立审批服务器的 IP 地址，端口默认为：8180，配置完毕后，点击连接测试，查看是否成功。服务器辅地址是为需配置外网的客户设计，将映射到外网的 IP 及端口输入即可，无需映射到外网的客户可不配置。注：旧客户升级到独立审批可勾选保留旧审批菜单栏，以便将旧审批流程导入独立审批流程。

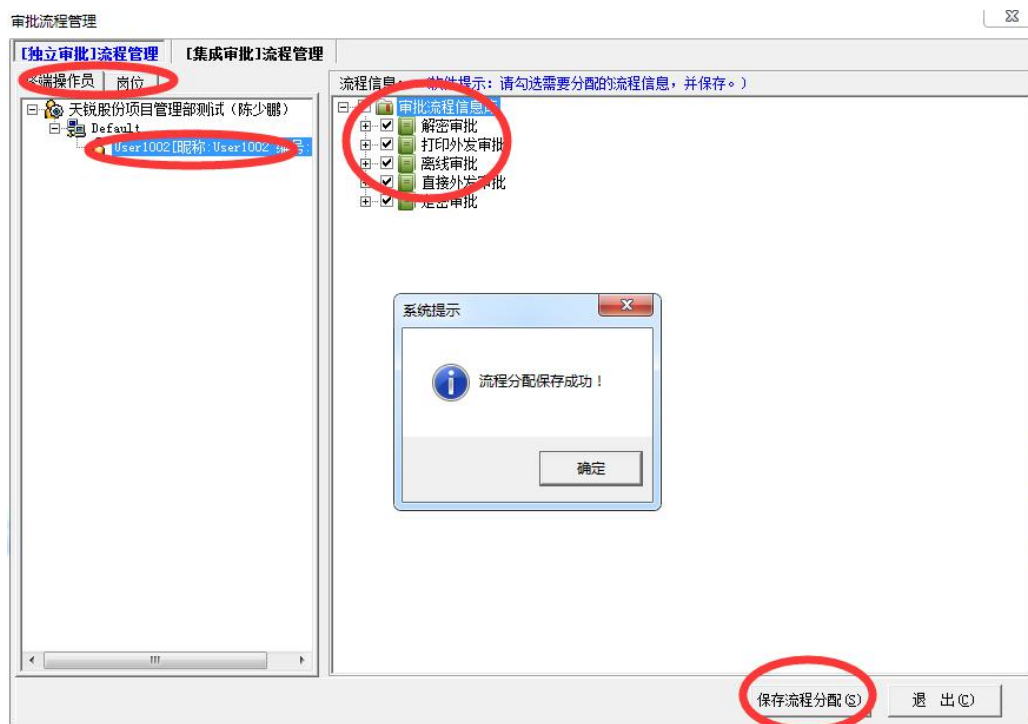


“审批岗位”：依次点击规则中心—操作员—岗位设置与分配，为操作员设置审批岗位。流程和审批人可以按岗位分配。具体表现为：可将一条流程分配给该岗位下的所有操作员。还可将岗位设置为审批人，该岗位下的所有操作员都能收到审批信息，有一人通过即可。

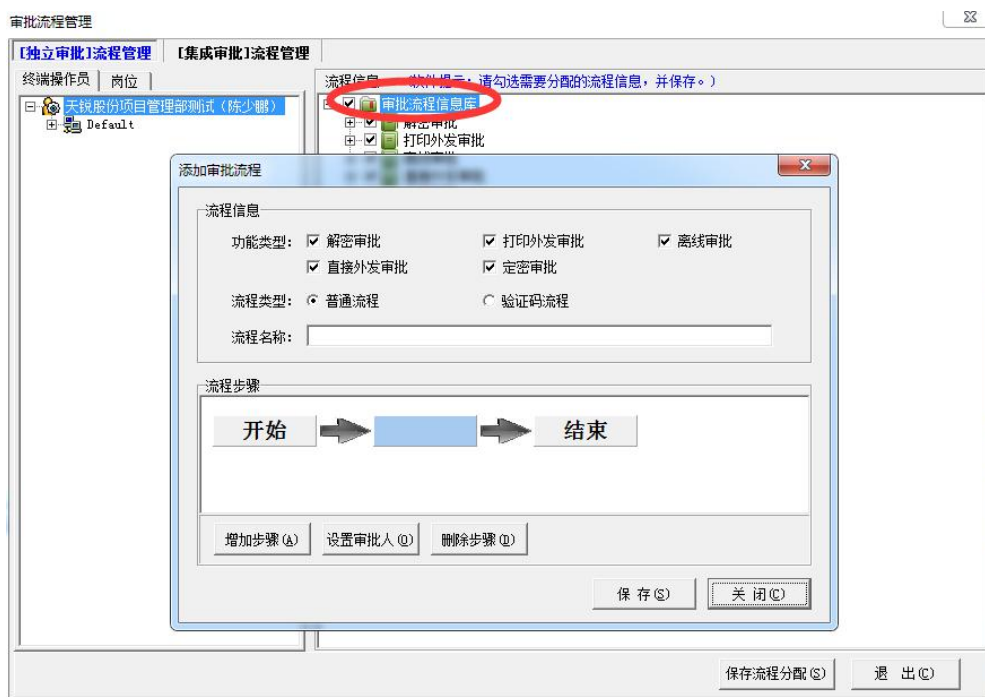


“审批流程管理”：开启独立审批后需重新为终端分配流程，依次点击审批流程管理—独立审批流程管理，可按终端或者岗位分配流程，选择对应终端或岗位勾选对应流程点击保存流程分

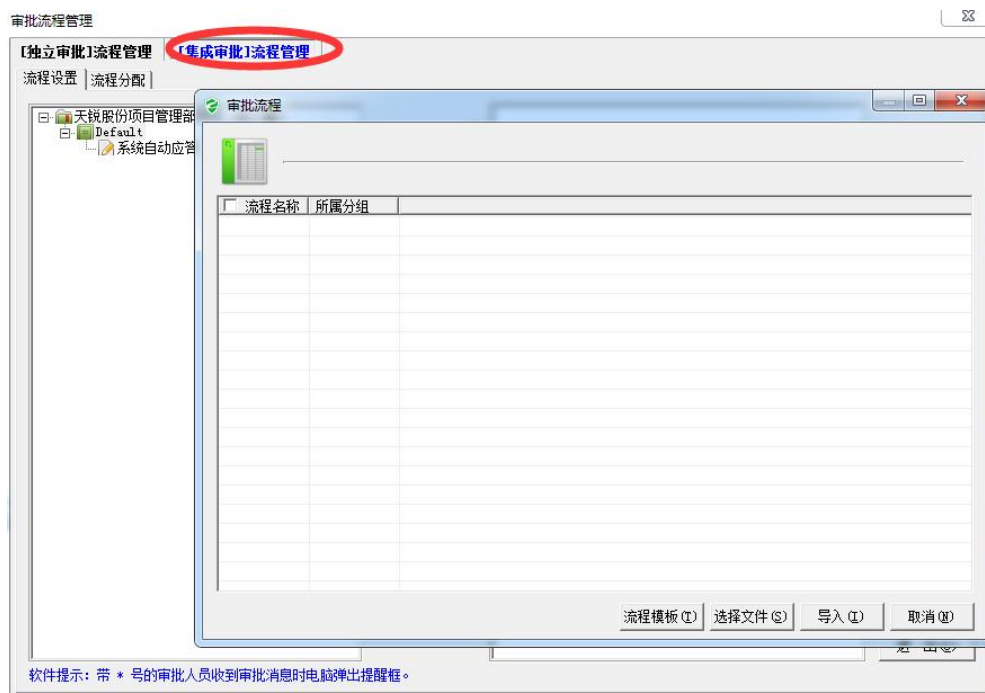
配即可。



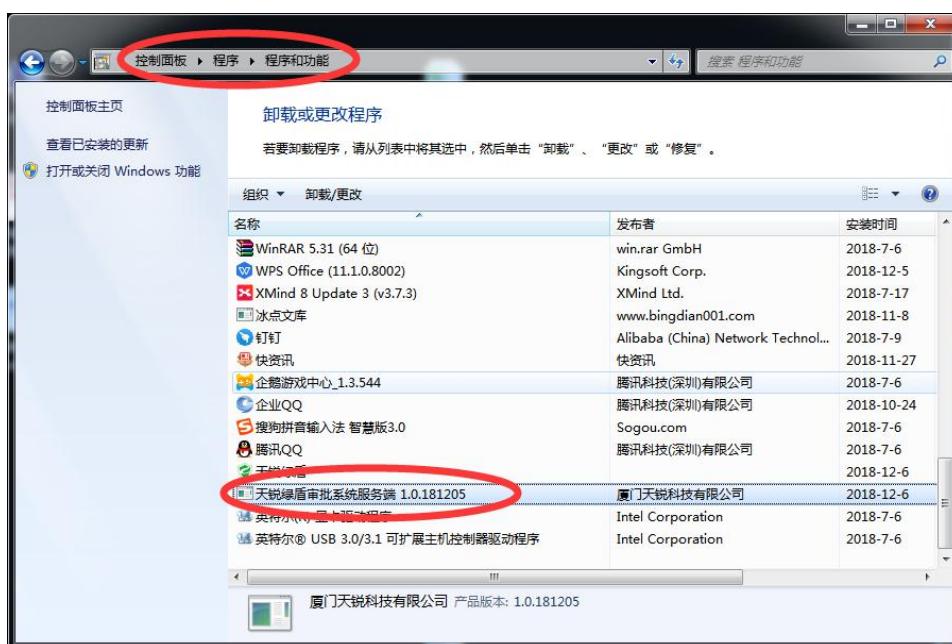
“新建审批流程”：右键审批流程信息库，选择新建流程，可按照需要新建审批流程。



“导入旧审批流程”：配置参数时选择保留旧审批菜单，点击集成审批流程管理分页，右键左侧流程列表，选择导出流程，勾选对应流程选择导出。点击独立审批流程管理分页，右键右侧流程信息表，选择导入流程，选择相应文件，点击导入即可。

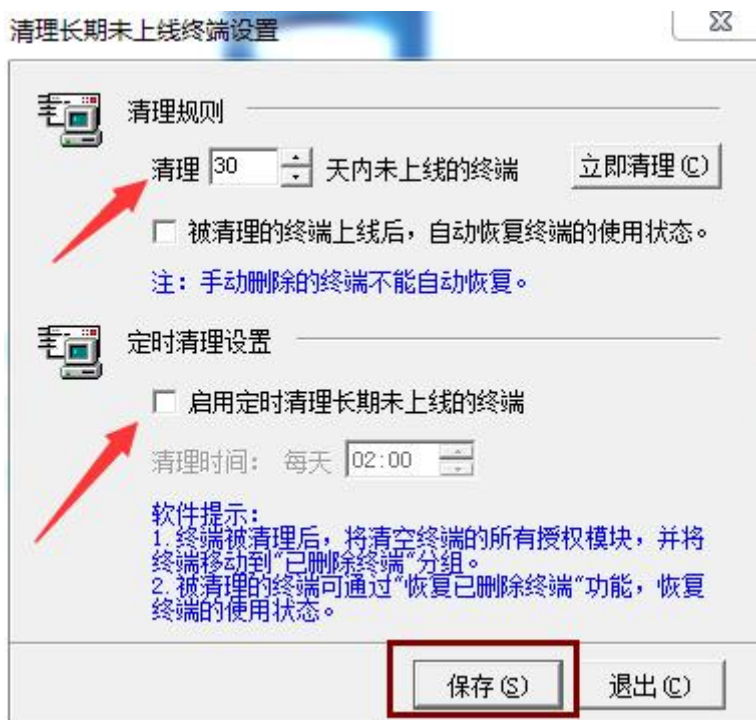
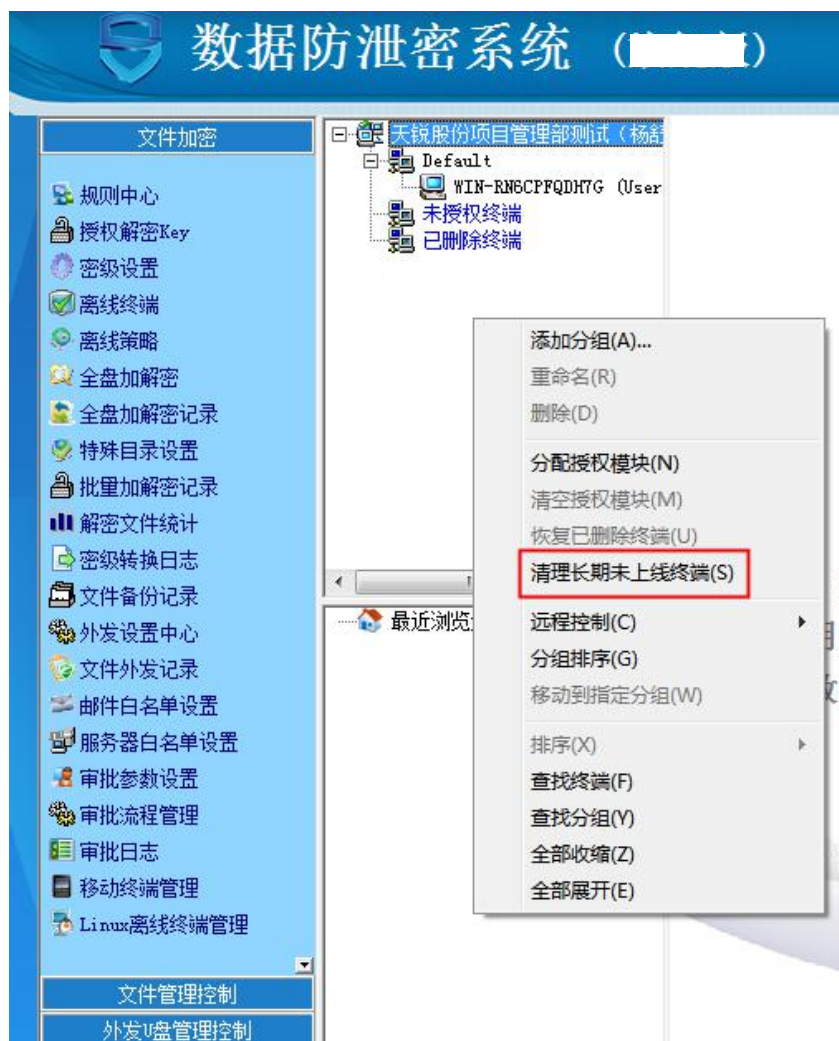


“卸载审批服务器”：如需卸载审批服务器，点击系统“控制台”——“卸载程序”选择天锐绿盾服务器并双击，即可进入卸载流程。卸载后，引擎将不可使用独立审批，配置的流程也将全部消失。

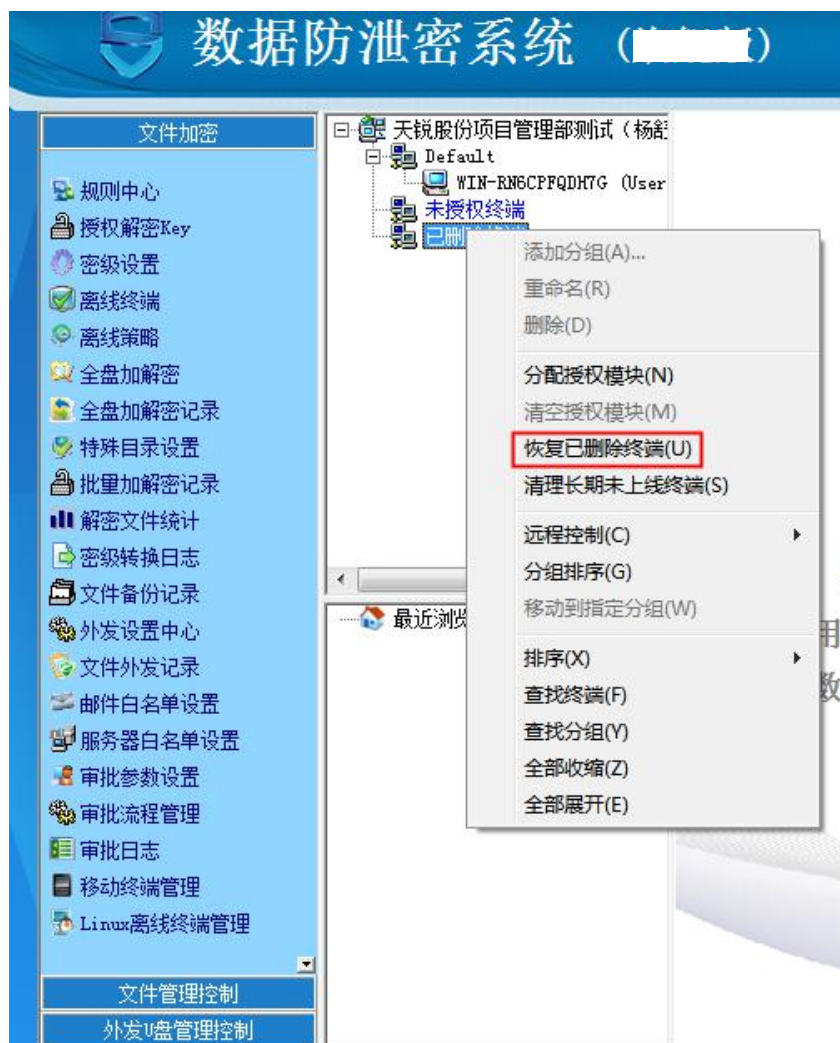


2.25 长期未上线终端管理

文件加密—终端列表中空白处右键选择“清理长期未上线终端”则弹出清理长期未上线终端设置弹窗，设置清理规则，即可清理符合规则的终端；如下图所示。

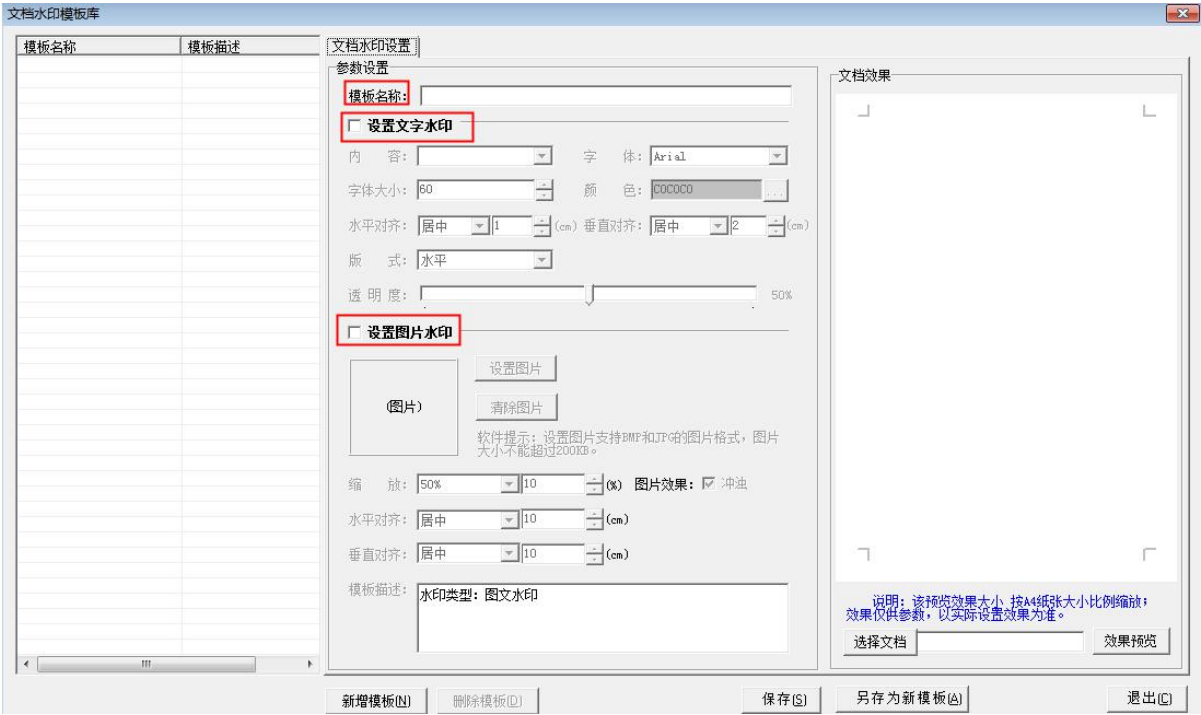


选中“已删除终端”右键点击弹窗中的“恢复已删除终端”即可恢复被删除终端，如下图所示。



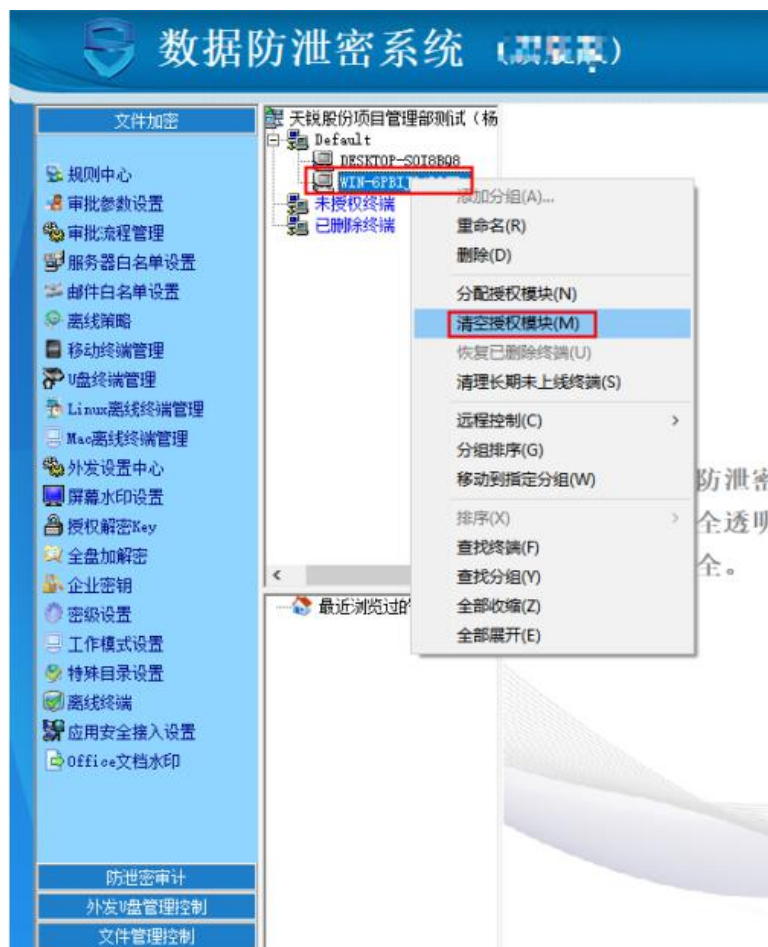
通过 word 文档水印设置,可以选择是否对申请及批量解密.docx 后缀文件,进行设置图片、文字水印。

在控制台的功能栏中选择“文件加密”-“word 文档水印”，弹出“文档水印模板库”窗口，在窗口中间设置文档水印的模板名称，文字水印的内容、字体大小、颜色和透明度等或图片水印的图片、缩放比例、水平对齐等，设置完成后，点击“保存”即可。也可对选中的模板进行删除和修改。如图所示：

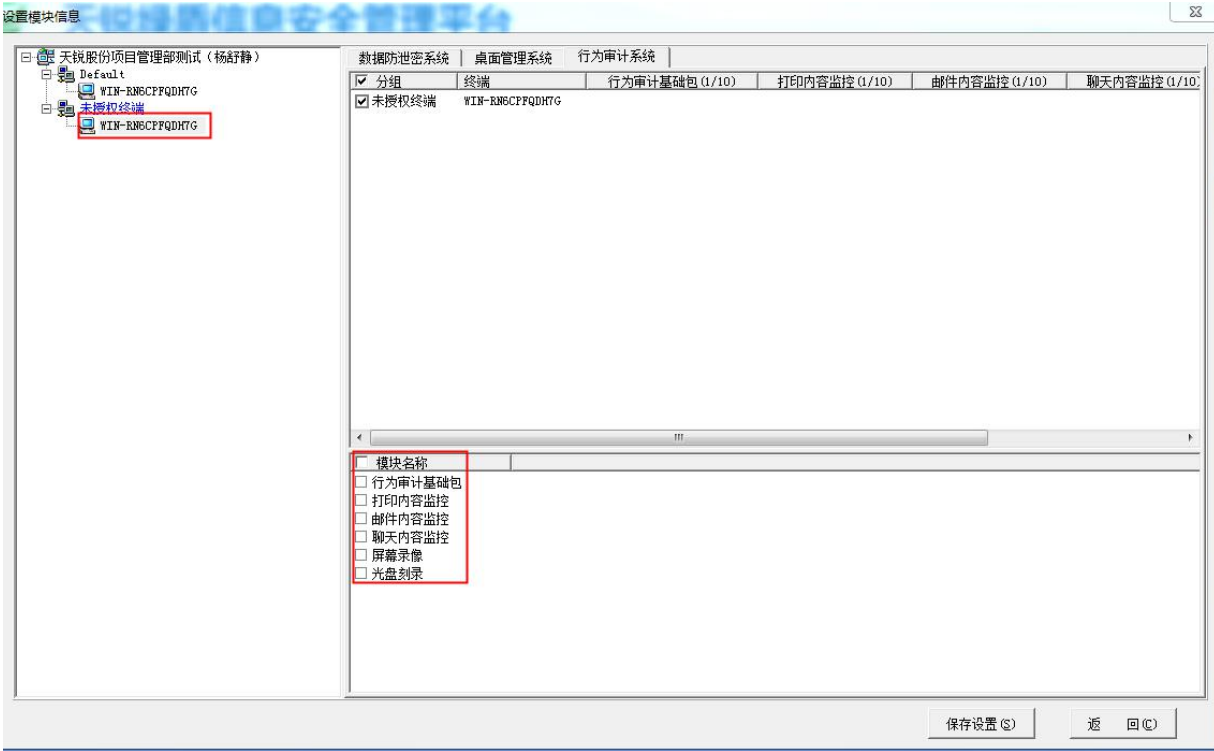


2.26 未授权终端

终端列表中选择要清空授权的终端右键选择“清空授权模块”则弹出[清空终端授权模块]确认设置弹窗，点击“清空模块”则该终端的所有模块权限被清空。如下图所示。

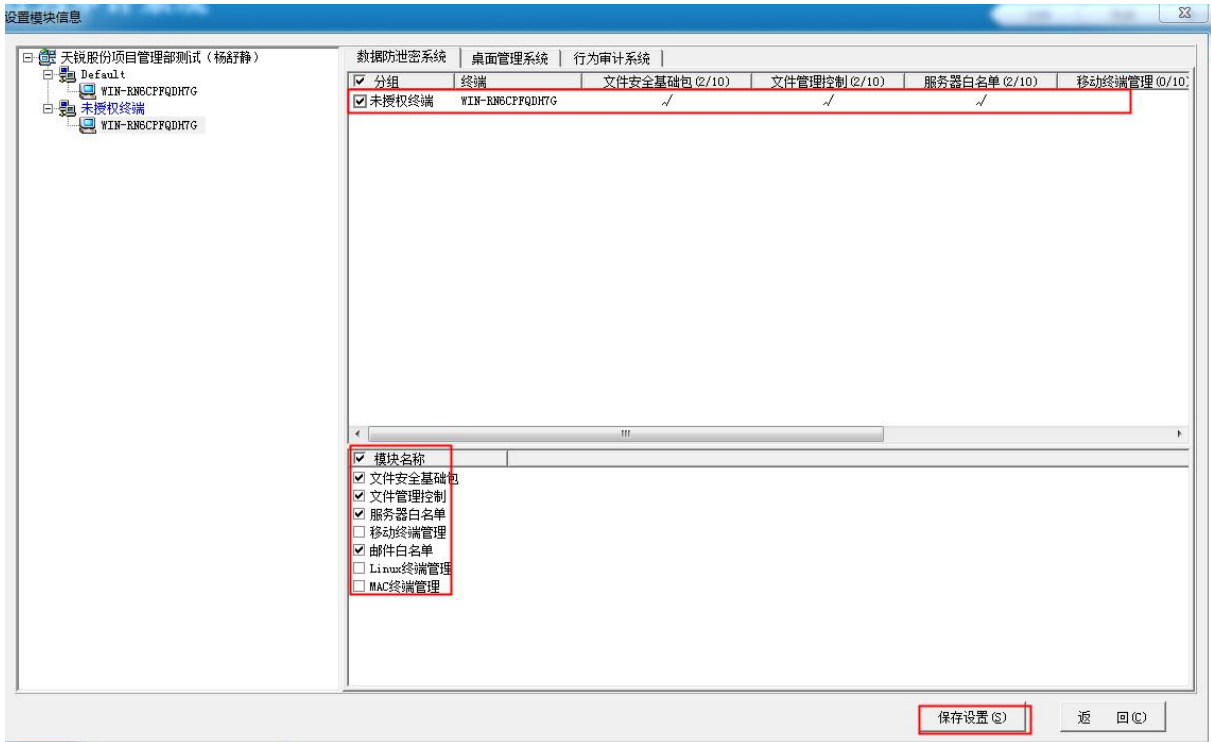
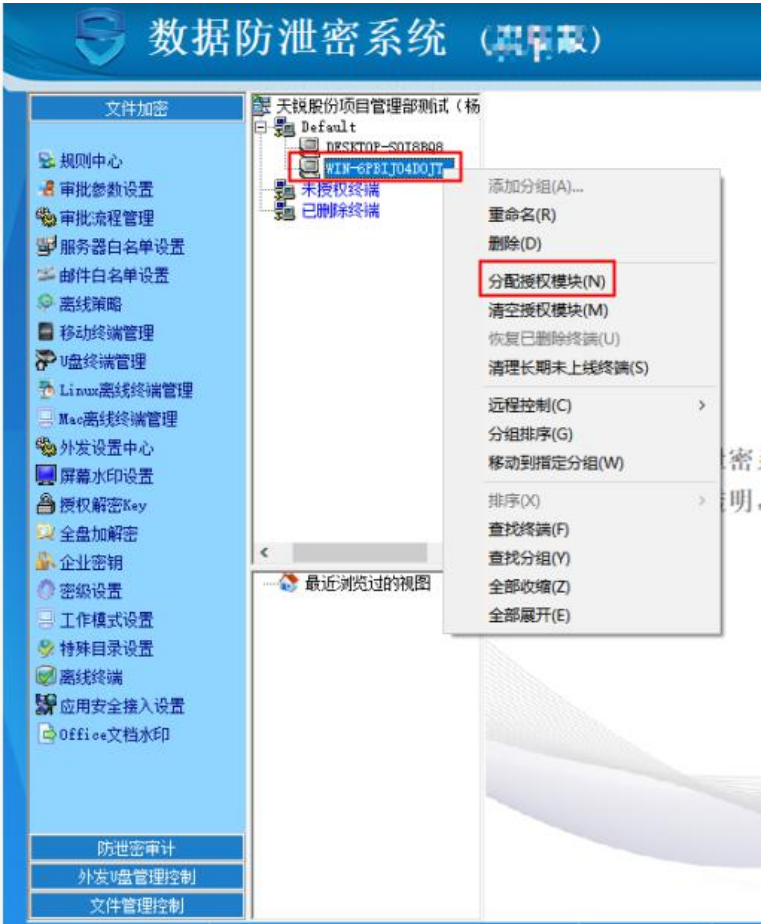


控制台-终端管理-设置模块信息界面取消终端所有模块勾选则该终端的所有模块授权也被情况即为未授权终端。如图所示。



被清空授权的终端只有重新分配授权才可以正常使用。

选中未授权的终端右键选择“分配授权模块”则弹出设置模块信息弹窗，分配该终端的模块点击保存设置即可正常使用。如图所示。



2.27 office 文档水印

设置文档水印内容，用户可自行选择打开 office 文档是否需要水印。

在控制台的功能栏选择“office 文档水印”-“文档水印模板信息管理”，将弹出“文档水印模板库”窗口。设置文档水印内容，包括水印添加时机、文字水印内容（水印内容、版式、字体大小、字体、颜色等文本属性），若需要增加图片水印则点击“高级设置”勾选“设置图片水印”进行图片水印的属性设置，选择需要加水印的文档，点击“保存”即可。关闭“文档水印模板库”窗口，退到“文档水印设置”界面，在左侧选择添加水印的终端，右侧中勾选水印的模板，点击“修改生效”即可。如下图：

